

福 井 大 学 審 査  
学位論文 [博士(工学)]

量子状態の識別問題

2013年3月

福井大学大学院工学研究科博士後期課程  
物質工学専攻 平成22年度入学

杉本 宏行

# 目次

第 1 章	序論	3
第 2 章	導入	7
2.1	量子ビット	7
2.2	量子エンタングルメント	9
2.3	POVM 測定	10
第 3 章	2 つの純粋状態の識別問題	12
3.1	Minimum-error discrimination	12
3.2	Unambiguous discrimination	14
第 4 章	2 つの純粋状態のエラーマージンのある識別問題	18
4.1	問題の定式化と解	18
4.2	Intermediate 領域	23
4.3	Single-state 領域	28
4.4	弱いエラーマージンと強いエラーマージン	30
4.5	混合状態に対する上限	32
第 5 章	3 つの純粋状態の minimum-error discrimination	35
5.1	問題の定式化	35
5.2	2 つの純粋状態の場合	36
5.3	生起確率が等しい qubit の 3 つの純粋状態の場合	40
5.3.1	外心が外周上を含む三角形の内部に存在する場合	42
5.3.2	外心が三角形の外部に存在する場合	46
5.3.3	例	48
5.4	一般の生起確率を持つ qubit の 3 つの純粋状態の場合	52
第 6 章	3 つの純粋状態の unambiguous discrimination	59
6.1	一般論	59
6.1.1	問題の定式化	59
6.1.2	Relaxed problem と状態の数の減少	61
6.1.3	Relaxed problem の双対問題	64
6.2	互いの内積が実数である場合	65
6.2.1	2 つの純粋状態の場合	65
6.2.2	3 つの純粋状態の場合	68
6.2.3	例	74

6.3	互いの内積が複素数である場合 . . . . .	77
6.4	解の一意性 . . . . .	80
<b>第 7 章</b>	<b>3 つの qubit のエラーマージンのある識別問題</b>	<b>83</b>
7.1	問題の定式化 . . . . .	83
7.2	Qubit の 3 つの対称な純粋状態の場合 . . . . .	85
7.2.1	Minimum-error 領域 . . . . .	87
7.2.2	Linear 領域と intermediate 領域 . . . . .	90
7.2.3	例 . . . . .	94
7.3	Qubit の 3 つの対称な混合状態の場合 . . . . .	95
<b>第 8 章</b>	<b>結論</b>	<b>96</b>
	謝辞	98
	参考文献	99
<b>付 録 A</b>	<b>Pauli 行列</b>	<b>102</b>
<b>付 録 B</b>	<b>三角形の外心</b>	<b>104</b>

# 第1章 序論

原子や分子、素粒子などの微視的世界の現象を説明する物理の基礎理論である量子力学では、状態の重ね合わせ、不確定性原理、測定の統計性、量子エンタングルメントなど古典力学にはない奇妙な性質がある。このような量子力学特有の性質を情報通信や情報処理の原理に応用するのが量子情報と呼ばれる分野である。

現在の情報処理では、ビット (bit) と呼ばれる 0 と 1 の集まりで情報すべてを表す。量子情報分野で、このビットに対応するのが、量子ビット (qubit) である。量子ビットは 2 つの基本的な状態を持つ物理系であり、例として、電子のスピン、光子の偏光などが挙げられる。量子ビットは  $|0\rangle$  と  $|1\rangle$  の 2 値だけでなく、 $|0\rangle$  と  $|1\rangle$  の状態を同時に含む重ね合わせの状態もとることができる。また、いくつかの量子系を部分系とする複合系では、量子エンタングルメントと呼ばれる特徴的な状態が見られる。例として、2 つの量子ビットからなる系を考える。その系のある状態に対して、ある基底で測定したとする。そのとき、1 つの量子ビットの測定結果が  $|0\rangle$  であったら、もう 1 つの量子ビットの測定結果も直ちに  $|0\rangle$  と決まるような状態が存在する。このように 1 つの量子ビットの測定結果が決定されると同時に、もう 1 つの量子ビットの測定結果も決定されるような状態を量子エンタングルメントと呼んでいる。あるいは、Einstein, Podolsky, Rosen らの思考実験に因んで EPR 相関などとも呼ばれる。

このような量子情報分野では、現在の情報通信や情報処理では実現不可能な技術、例えば、スーパーコンピュータの性能を凌駕する超並列・高速情報処理が可能な量子コンピュータや絶対に盗聴不可能な量子暗号通信などが実現される可能性があることが証明されている。現在、インターネット上で広く用いられるのが RSA 暗号などに代表される公開鍵による暗号である。それらの暗号の安全性は桁数の大きい合成数の素因数分解の困難さに依存しており、もし、超高速の計算機があれば、原理的に解読することは可能である。一方、量子暗号通信の安全性は物理の基本原則に依存しているため、解読は絶対に不可能である。近年、これらの技術を実現するために、世界の様々な分野の研究者たちによって、盛んに研究が行われている。しかしながら、外部環境との相互作用によって量子系の干渉が失われる量子デコヒーレンスが原因で量子エンタングルメントを長時間、維持することが難しいなどの未解決問題も多い。

本研究では、量子情報分野において、最も基本的で重要な研究課題である量子状態の識別問題を取り上げる。情報通信を行う上で、モノを識別することは非常に重要なことである。しかしながら、量子力学では、一般に、異なる非直交の量子状態を誤りなく完全に識別することは不可能である。それは量子状態を測定しても、その測定結果は確率的にしか現れず、測定された系の状態は壊れてしまうからである。そこで、考えられる問題は様々な設定で量子状態を識別する最適な方法を見つけることである [1–3]。もし、それが可能となれば、量子暗号通信を実現するための通信システムの受信過程を最適化

することに非常に大きな寄与をもたらすであろうと考えられる。

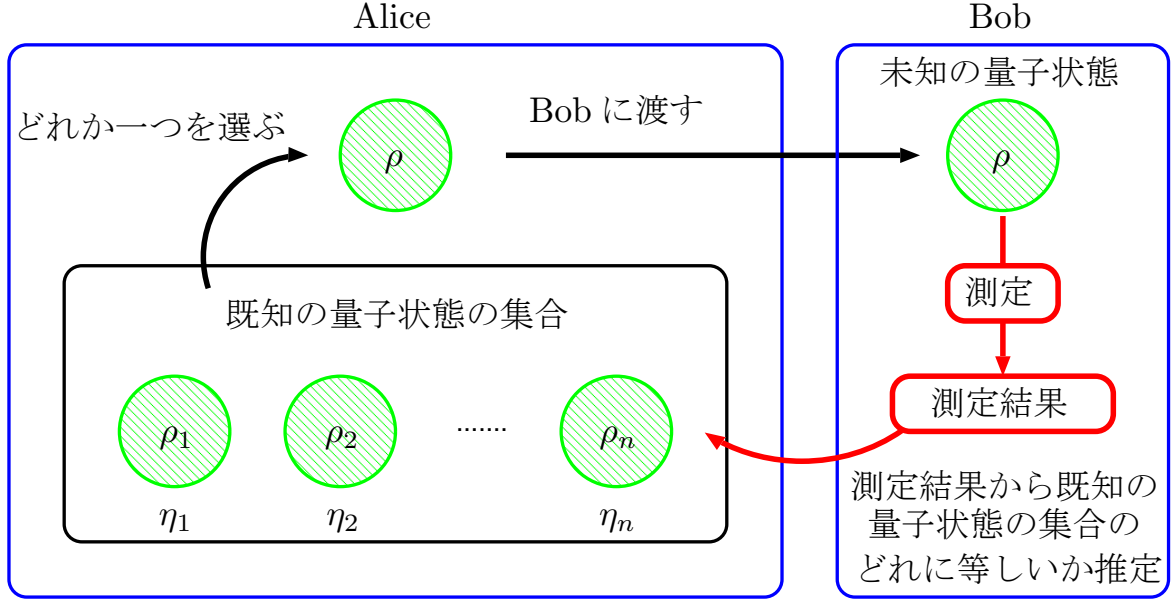


図 1.1: 量子状態の識別問題

量子状態の識別問題 [1] を簡単に理解するために、量子情報分野の多くの概念と同様、Alice と Bob の両者間のゲームの比喻が用いられる。まず、Alice は両者が知っている量子状態の集合  $\{\rho_i\}_{i=1}^n$  から 1 つの状態  $\rho$  を選び、Bob に渡す。Bob の課題は与えられた状態  $\rho$  に対して、測定を行い、その測定結果から  $\rho$  が集合  $\{\rho_i\}_{i=1}^n$  のどれに等しいかを言い当てることである。このような量子状態の識別問題を考える際、よく研究されている 2 つの設定がある。1 つは識別が間違えることに対して何の制限も課さないで、識別成功確率を最大にする設定である。結果的に、これは識別間違い確率を最小にするので、minimum-error discrimination と呼ばれる [2]。もう 1 つは unambiguous discrimination と呼ばれ、識別に間違いが許されない。しかし、その代わりに識別が成功する可能性がない場合、“わからない”という推定を許容し、識別成功確率を最大にする設定である [4–8]。その他にも、いくつかの興味深い設定が提案されている。その 1 つが maximum-confidence measurement である [9–11]。また、“わからない”と推定する割合を一定にし、識別成功確率を最大にする設定も考えられている [12–15]。さらに、別の設定として、識別間違い確率に対してエラーマージンと呼ばれるある有限のマージン  $m$  を越えてはならないという条件を課して、識別成功確率を最大にする設定が考えられている [16, 17]。  $m = 0$  の場合、unambiguous discrimination の設定に対応している。一方、  $m = 1$  の場合、minimum-error discrimination の設定に対応していることは明らかである。この設定はエラーマージン  $m$  を操作することで、minimum-error discrimination の設定と unambiguous discrimination の設定を連続的に補間することができる。この設定において、Touzel, Adamson, Steinburg らは射影測定と POVM (Positive Operator-Valued Measure) 測定の数値解析の結果を比較した [16]。さらに、林, 橋本, 堀邊らは等しい生起確率を持つ 2 つの純粋状態の場合を分析し、閉じた形式で解析的に最大識別成功確率を与えた [17]。本研究では、一般の生起確率の場合に拡張する [18]。新し

い特徴として、生起確率とエラーマージンによって構成される 2 次元パラメータ空間は 3 つの領域に分類され、その領域によって最適な測定のタイプは異なることがわかった。もし、エラーマージンが十分に大きいならば、識別間違い確率に対する制限は作用しない。そのとき、最適な測定は minimum-error discrimination のそれであることが予期される。このような領域を minimum-error 領域と呼ぶ。一方、エラーマージンが小さいときにはどのようなことが起こるだろうか。それを見るためには unambiguous discrimination ( $m = 0$ ) の結果を思い出すとよい。もし、1 つの状態の生起確率が十分に小さいならば、最適な測定はこの状態を除外した 2 つの結果を生み出す。これは一般のエラーマージンに対してもパラメータ空間内の single-state 領域と呼ばれる領域で起こることが予期される。そして、intermediate 領域は 3 つの測定結果の確率が 0 でない領域である。さらに、識別間違い確率に課されるエラーマージンのタイプには 2 つのタイプが考えられる。1 つは平均の間違い確率に対する制限であり、もう 1 つは条件付き間違い確率に対する制限である。これら 2 つの制限のタイプの最大識別成功確率のあいだにある関係を証明する。これにより、2 つの純粋状態の場合、どのような設定でも完全に解析解が得られるようになった。しかしながら、識別される状態が 2 つ以上の複数個の場合に関しては数多くの研究がなされているにもかかわらず、minimum-error discrimination や unambiguous discrimination といった標準的な設定でさえ解析的な解を得ることは容易ではない [19–31, 39]。

最近、Samsonov によって qubit の純粋状態の minimum-error discrimination が詳しく分析された [22]。そこで、生起確率が等しい qubit の 3 つの純粋状態の場合に完全な解析解を与えた。本研究では、別の方法として、主問題から導かれた双対問題を解くことで解析的な解を与える [32]。そのとき、識別される 3 つの状態の Bloch ベクトルの終点が成す三角形の外心が最適な解の構成に重要な役割を果たす。さらに、この解析を一般の生起確率の場合にも拡張する。また、3 つの純粋状態の unambiguous discrimination は一般論を扱ういくつかの論文の中で応用の 1 つとして考えられている。しかし、3 つの純粋状態の場合でも限られた特別な場合にだけしか完全な解析解は得られていない。ここで、解析解が得られている例をいくつか挙げる。1 つめは等しい生起確率を持ち、ある同一の unitary 演算子によって生成された対称な状態の場合である [25]。2 つめは実数である互いの内積の 3 つのうちの 2 つが等しく、生起確率が等しい場合である [27]。3 つめは一般の生起確率を持つ 3 つの純粋状態で互いの内積の 1 つが 0 である場合である [31]。本研究では、一般の生起確率を持ち、互いの内積が実数である 3 つの純粋状態の unambiguous discrimination に対する完全な解析解を与える [33]。そして、互いの内積が一般の複素数の場合に拡張する。Unambiguous discrimination での最適な測定では与えられた状態のうちのいくつかの状態であると同定する確率は 0 であるときがある。この事象については論文内で詳しく分析する。さらに、本研究では、3 つの qubit の対称な状態のエラーマージンのある識別問題についても考察する [34]。まず、qubit の 3 つの対称な純粋状態の場合について分析する。そのとき、最適な測定はエラーマージンの値によって 3 つのタイプに分類される。そして、任意のエラーマージンに対して完全に解析解が得られた。また、qubit の 3 つの対称な混合状態の場合についても分析する。最近、この設定に関連する 2 つの新しい仕事 [35, 36] が発表された。この 2 つの仕事では、“わからない”と推定する結果を一定の割合にする設定を対称な状態の場合に適用し、そ

の結果がエラーマージンのある識別問題に対する解に変換することができることを議論している。

まず、初めに第2章では、量子情報分野の導入として、最も簡単な量子系である qubit や量子多体系において現れ、古典的確率では説明できない相関である量子エンタングルメント、量子情報分野において量子系を測定するのに一般的な測定である POVM 測定についてまとめる。第3章では、量子状態の識別問題を考える上で標準的な minimum-error discrimination と unambiguous discrimination の設定それぞれについて、2つの純粋状態の場合を考察し、最大識別成功確率を導出する。第4章では、一般の生起確率を持つ2つの純粋状態の場合にエラーマージンのある識別問題の設定を分析し、最大識別成功確率を導出する。さらに、2つの識別間違い確率に対する制限のタイプの最大識別成功確率のあいだにある関係を証明する。また、2つの混合状態の場合に対する成功確率の上限が純粋状態の場合の最大識別成功確率によって簡単に与えられることを示す。第5章では、qubit の3つの純粋状態の minimum-error discrimination を考察する。まず、生起確率が等しい場合について分析し、最大識別成功確率を導出する。そのとき、識別される3つの qubit の Bloch ベクトルの終点が成す三角形の外心が最適な解析解を構成するために重要な役割を果たすことを証明する。さらに、この結果を一般の生起確率の場合に拡張する。第6章では、3つの純粋状態の unambiguous discrimination について考察する。まず、一般論として、 $n$  個の純粋状態の unambiguous discrimination について定式化する。そこで、ある制限を緩和した問題を考えることが非常に有用であることを証明する。さらに、その緩和された問題において、ある同定確率が0になる条件を明確にし、識別される状態が  $(n - 1)$  個の識別問題に変換されることも証明する。具体的に、2つの純粋状態の場合に、この戦略を適用し、先行研究や3.2節で得られた結果と一致することを示す。そして、互いの内積が実数である3つの純粋状態の場合を分析し、完全な解析解を導出する。お互いの内積が一般の複素数の場合について拡張することも議論する。第6章の最後に、 $n$  個の純粋状態の unambiguous discrimination の解は一意的に決まることも示す。第7章では、3つの qubit のエラーマージンのある識別問題を考察する。まず、識別される状態が  $n$  個のエラーマージンのある識別問題について定式化する。そして、qubit の3つの対称な純粋状態の場合を分析し、最大識別成功確率を導出する。さらに、この結果を qubit の3つの対称な混合状態の場合に拡張する。最後に第8章では、本研究のまとめとして結論を述べる。

## 第2章 導入

量子状態の識別問題を考える前に、量子情報分野の導入として、量子情報の最小単位でもある量子ビットや量子多体系において現れる量子エンタングルメント、量子情報分野では一般的な測定である POVM 測定についてまとめる。

### 2.1 量子ビット

現在の情報通信や情報処理では、ビット (bit) と呼ばれる 2 進数、つまり、0 と 1 の集まりによって情報すべてを表す。一方、量子情報分野において、このビットに対応するのが量子ビット (quantum bit)、あるいは略して qubit と呼ばれる概念である。Qubit は 2 つの基本的な状態を持つ物理系 (2 準位系) であり、例として、電子のスピン、光子の偏光などが挙げられる。また、qubit は通常のビットとは異なり、 $|0\rangle$  と  $|1\rangle$  の 2 値だけでなく、 $|0\rangle$  と  $|1\rangle$  の状態を同時に含むような重ね合わせの状態もとることができる。

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (2.1)$$

ここで、 $\alpha, \beta$  は複素数である。この  $|\psi\rangle$  に対して正規直交基底  $\{|0\rangle, |1\rangle\}$  に関する測定を行うと、確率  $|\alpha|^2$  で 0、または確率  $|\beta|^2$  で 1 という結果が得られる。全確率の和は 1 であることから、 $\alpha, \beta$  は

$$|\alpha|^2 + |\beta|^2 = 1, \quad (2.2)$$

を満たさなければならないことは明らかである。これは幾何学的解釈において、qubit のノルム (長さ) が 1 に規格化 (正規化) される条件である。したがって、一般に qubit は 2 次元複素ベクトル空間の単位ベクトルを表す。

単一 qubit を考える上で、非常に有用な幾何学的表現がある。(2.1) 式によって与えられた状態  $|\psi\rangle$  は (2.2) 式で規格化されているので、次のように書き換えることができる。

$$|\psi\rangle = e^{i\gamma} \left( \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right), \quad (2.3)$$

ここで、 $\theta, \varphi$ , および、 $\gamma$  は実数である。ただし、右辺の最初の因子  $e^{i\gamma}$  はグローバル因子と呼ばれ、観測可能な効果をもたらさないので無視することができる。それゆえ、 $|\psi\rangle$  は実効的に次のように記述される。

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle. \quad (2.4)$$



図 2.1 に示すように  $|\psi\rangle$  は 3 次元単位球面上の点として定義される. この球面は Bloch 球と呼ばれ, 単一 qubit を視覚的にとらえるのに便利な方法である. 単一 qubit に対する多くの操作はこの Bloch 球上の描像で記述される. ただし, Bloch 球は多 qubit に対して簡単に一般化することはできないので注意しなければならない.

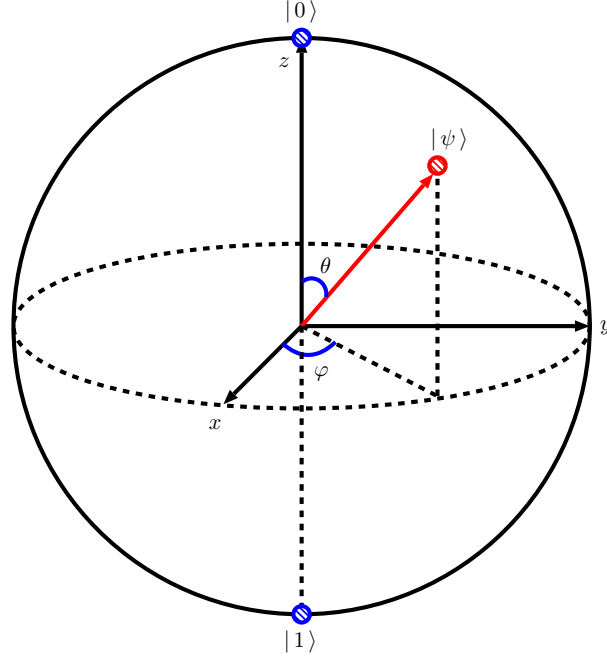


図 2.1: Bloch 球

また, 図 2.1 のように原点を始点とし, 3 次元単位球面上の点  $|\psi\rangle$  を終点とする単位ベクトル  $\mathbf{n}$  は Bloch ベクトルと呼ばれ, 次のような 3 成分で表示される.

$$\mathbf{n} = (\sin \theta \cos \varphi, \sin \theta \sin \varphi, \cos \theta). \quad (2.5)$$

さらに, この Bloch ベクトルを用いた 2 つの関係式がある. 1 つは qubit の内積公式であり, 次のように導出される.

$$\begin{aligned} |\langle \psi | \psi' \rangle|^2 &= \left| \left( \cos \frac{\theta}{2} \langle 0 | + e^{-i\varphi} \sin \frac{\theta}{2} \langle 1 | \right) \left( \cos \frac{\theta'}{2} | 0 \rangle + e^{i\varphi'} \sin \frac{\theta'}{2} | 1 \rangle \right) \right|^2 \\ &= \left| \left( \cos \frac{\theta}{2} \cos \frac{\theta'}{2} + \cos(\varphi - \varphi') \sin \frac{\theta}{2} \sin \frac{\theta'}{2} \right) - i \left( \sin(\varphi - \varphi') \sin \frac{\theta}{2} \sin \frac{\theta'}{2} \right) \right|^2 \\ &= \frac{1}{2} [1 + \cos \theta \cos \theta' + \sin \theta \sin \theta' \cos(\varphi - \varphi')] \\ &= \frac{1 + \mathbf{n} \cdot \mathbf{n}'}{2}, \end{aligned} \quad (2.6)$$

ここで,  $\mathbf{n}, \mathbf{n}'$  はそれぞれ状態  $|\psi\rangle, |\psi'\rangle$  の Bloch ベクトルである.

もう1つは qubit の外積公式であり, 次のように導かれる.

$$\begin{aligned}
|\psi\rangle\langle\psi| &= \left( \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \right) \left( \cos\frac{\theta}{2}\langle 0| + e^{-i\varphi}\sin\frac{\theta}{2}\langle 1| \right) \\
&= \cos^2\frac{\theta}{2}|0\rangle\langle 0| + e^{-i\varphi}\cos\frac{\theta}{2}\sin\frac{\theta}{2}|0\rangle\langle 1| + e^{i\varphi}\cos\frac{\theta}{2}\sin\frac{\theta}{2}|1\rangle\langle 0| + \sin^2\frac{\theta}{2}|1\rangle\langle 1| \\
&= \frac{1}{2} \begin{bmatrix} 1 + \cos\theta & (\cos\varphi - i\sin\varphi)\sin\theta \\ (\cos\varphi + i\sin\varphi)\sin\theta & 1 - \cos\theta \end{bmatrix} \\
&= \frac{1 + \mathbf{n} \cdot \boldsymbol{\sigma}}{2}, \tag{2.7}
\end{aligned}$$

ここで,  $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$  は Pauli 行列である. Pauli 行列については付録 A で詳しくまとめているので参照する. これら2つの関係式は次節以降, 非常に有用な表現であるので覚えておく.

## 2.2 量子エンタングルメント

複数の qubit からなる量子系において, どの系にも興味がある場合, それらの系をまとめて記述する必要がある. まず, 2つの qubit から成る量子系を考える. 例えば, 1つめの qubit が状態  $|0\rangle$  にあり, 2つめの qubit が状態  $|1\rangle$  にあるとき, この量子系の全系は次のように記述することができる.

$$|0\rangle \otimes |1\rangle \equiv |0\rangle|1\rangle \equiv |01\rangle.$$

したがって, 2つの qubit から成る量子系は次のような4つの基本的な状態を持つ.

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle.$$

そして, これら4つの状態を重ね合わせた状態もとることができる.

$$|\Phi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle.$$

さて, 次のような2つの qubit から成る状態  $|\Psi\rangle$  が与えられたとしよう.

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2.8}$$

この  $|\Psi\rangle$  に対して, 基底  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$  に関する測定を行うと, 確率  $1/2$  で  $00$ , または確率  $1/2$  で  $11$  という結果を得る. 今, Alice が1つめの qubit を持ち, Bob が2つめの qubit を持って互いに遠く離れた場所にいたとする. Alice と Bob はそれぞれが持つ qubit に対して基底  $\{|0\rangle, |1\rangle\}$  に関する測定を行うと, Alice の測定結果が  $0$  ならば, Bob の測定結果も必ず  $0$  である. 一方, Alice の測定結果が  $1$  ならば, Bob の測定結果も必ず  $1$  である. このように部分系に対して2つの測定結果が絡み合っている状態をエンタングルした状態, あるいは Einstein, Podolsky, Rosen の思考実験に因んで EPR 相関と呼ばれる.

## 2.3 POVM 測定

POVM(Positive Operator-Valued Measure) 測定は物理を学ぶ多くの人にとって、あまり馴染みがないかもしれない。しかしながら、測定後の状態にはあまり興味がなく、測定の統計のみが重要である場合、例えば、実験結果を得るために系を 1 回だけ測定する場合、量子測定の見通しを簡単に得る直観的な方法として便利である。

まず、状態  $|\psi\rangle$  にある量子系に対して、測定演算子  $M_m$  で記述される測定を行うとする。このとき、測定結果  $m$  を得る確率は  $p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$  で与えられる。そこで、次式で演算子  $E_m$  を定義する。

$$E_m \equiv M_m^\dagger M_m, \quad (2.9)$$

ここで、 $E_m$  は  $\sum_m E_m = I$  および  $p(m) = \langle \psi | E_m | \psi \rangle$  を満たす半正定値演算子である。半正定値演算子とは Hermite であり、すべての固有値が実数で負でない演算子として定義される。そして、それは次のように記述される。

$$E_m \geq 0.$$

この記述の仕方は半正定値演算子を定義する簡単な方法として、本論文でも頻繁に登場するので覚えておく。以上から、演算子の集合  $E_m$  があれば、異なる測定結果の確率を決定することができる。演算子  $E_m$  は測定に関する POVM 要素 (POVM element), その完全集合である  $\{E_m\}$  を POVM と呼ぶ。

POVM の例として、測定演算子  $P_m$  で記述される射影測定を考える。ここで、 $P_m$  は  $P_m P_{m'} = \delta_{mm'} P_m$  および  $\sum_m P_m = I$  を満たす射影演算子である。この測定では、 $E_m \equiv P_m^\dagger P_m = P_m$  であるから、全 POVM 要素が測定演算子自身に等しい。したがって、POVM 測定は射影測定を含んだより一般的な測定であることがわかる。また、POVM 測定は測定する系に補助系を加えて、その全系に対して射影測定を行うという構造となっている。

これまで、POVM の例として射影測定を見てきたが、特に POVM の有用性はあまり見られなかった。次の例では、POVM が量子計算や量子情報における我々の直観を導く役割を果たすことがわかる。まず、Alice が Bob に次のような 2 つの状態  $|\psi_1\rangle, |\psi_2\rangle$  のどちらかに準備された qubit を与えるとする。

$$\begin{aligned} |\psi_1\rangle &= |0\rangle, \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \end{aligned}$$

Bob は与えられた状態に対して次のような射影演算子によって射影測定を行う。

$$\begin{aligned} P_1 &\equiv |\psi_1\rangle\langle\psi_1|, \\ P_2 &\equiv I - P_1. \end{aligned}$$

このとき、識別が間違える確率はそれぞれ  $\langle \psi_2 | P_1 | \psi_2 \rangle = |\langle \psi_1 | \psi_2 \rangle|^2$ ,  $\langle \psi_1 | P_2 | \psi_1 \rangle = 0$  で与えられる。このように射影測定では、測定演算子をどのように選んでも、この 2 つの

識別間違い確率を同時に 0 にすることはできない。つまり、射影測定では状態を完全に信頼度よく識別することは不可能である。

では、Bob が行う測定が POVM 測定ならば、どうだろうか。次のような 3 つの要素を持つ POVM  $\{E_1, E_2, E_3\}$  を考える。

$$E_1 \equiv \frac{\sqrt{2}}{1 + \sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2}, \quad (2.10)$$

$$E_2 \equiv \frac{\sqrt{2}}{1 + \sqrt{2}} |1\rangle\langle 1|, \quad (2.11)$$

$$E_3 \equiv I - E_1 - E_2. \quad (2.12)$$

これら 3 つの演算子が完全性関係  $\sum_m E_m = I$  を満たす半正定値演算子であることは明らかである。例えば、Bob に状態  $|\psi_1\rangle = |0\rangle$  が与えられたとすると、Bob は POVM  $\{E_1, E_2, E_3\}$  で記述される測定を行う。識別間違い確率  $\langle \psi_1 | E_2 | \psi_1 \rangle = 0$  を満たすように  $E_2$  をうまく選んだので、 $E_2$  の結果を得る確率は 0 である。したがって、もし、測定結果が  $E_2$  ならば、Bob は受け取った状態が  $|\psi_2\rangle$  であると識別できる。同様に、もし、測定結果が  $E_1$  ならば、Bob は受け取った状態が  $|\psi_1\rangle$  であると識別できる。しかし、時には測定結果  $E_3$  を得るだろうが、このときには受け取った状態を識別することに関して何も推定できないので、“わからない”と言ってしまえばよい。ここで、肝心なことは Bob が受け取った状態の識別を決して誤らないことである。したがって、“わからない”という推定を許容することでこの絶対的确实性を得ることができる。

このように識別に間違いが許されない代わりに“わからない”という推定を許容するという設定は unambiguous discrimination と呼ばれ、量子状態の識別問題において、標準的な問題設定の 1 つである。今、注意すべきことはここで用いた POVM が unambiguous discrimination の設定で 2 つの状態を識別するのに最適であるとは言えないことである。2 つの純粋状態の unambiguous discrimination に対する最適な POVM は 3.2 節で与える。

## 第3章 2つの純粋状態の識別問題

量子状態の識別問題を考える上で、2つの設定がよく研究されている。1つは識別が間違えることに何の制限もしないで識別成功確率を最大にする設定である。これは結果的に識別間違い確率を最小にするので、minimum-error discrimination と呼ばれる。もう1つは unambiguous discrimination と呼ばれ、識別に間違いは許されない。その代わりに識別が成功する可能性がない場合に”わからない”という推定を許容して識別成功確率を最大にする。本章では、一般の生起確率  $\eta_i$  を持つ2つの純粋状態  $\rho_i = |\phi_i\rangle\langle\phi_i|$  ( $i = 1, 2$ ) の場合にこれら2つの設定についてそれぞれ分析する。

### 3.1 Minimum-error discrimination

Minimum-error discrimination の設定では、識別が間違えることに何の制限もしないで、識別成功確率を最大にする。そのとき、測定は状態  $|\phi_1\rangle, |\phi_2\rangle$  によって張られる2次元部分空間上の POVM で記述され、2つの要素  $\{E_1, E_2\}$  から構成される。要素  $E_i$  は測定結果1を得れば、与えられた状態は  $\rho_1$  であると推定し、測定結果2を得れば、与えられた状態は  $\rho_2$  であると推定することを意味する。さらに、 $E_1, E_2$  は POVM 要素であることから、次のような条件を満たさなければならない。

$$E_1 \geq 0, \quad E_2 \geq 0, \quad (3.1a)$$

$$E_1 + E_2 = I, \quad (3.1b)$$

与えられた状態が  $\rho_i$  ( $i = 1, 2$ ) であり、測定結果が  $\mu$  である同時確率は  $P_{\rho_i, E_\mu}$  によって表される。そして、 $P_{\rho_i, E_\mu}$  は次のように与えられる。

$$P_{\rho_i, E_\mu} = \eta_i \text{tr}[E_\mu \rho_i].$$

したがって、識別成功確率  $p_o$  は次のように与えられる。

$$p_o = \eta_1 \text{tr}[E_1 \rho_1] + \eta_2 \text{tr}[E_2 \rho_2]. \quad (3.2)$$

今、 $|\phi_1\rangle$  と  $|\phi_2\rangle$  の張る2次元部分空間を考えているので、状態  $\rho_i$  は Bloch ベクトルを用いて、次のように表すことができる。

$$\rho_i = |\phi_i\rangle\langle\phi_i| = \frac{1 + \mathbf{n}_i \cdot \boldsymbol{\sigma}}{2} \quad (i = 1, 2).$$

さらに, POVM 要素  $E_1, E_2$  も 2 次元部分空間上の Hermite 演算子であるので, 次のように表すことができる.

$$E_1 = \alpha + \beta \cdot \sigma, \quad E_2 = I - E_1 = 1 - \alpha - \beta \cdot \sigma,$$

ここで,  $\sigma$  は Pauli 行列である.

したがって, 識別成功確率  $p_o$  は次のように書き換えられる.

$$\begin{aligned} p_o &= \eta_1 \text{tr} \left[ (\alpha + \beta \cdot \sigma) \left( \frac{1 + \mathbf{n}_1 \cdot \sigma}{2} \right) \right] + \eta_2 \text{tr} \left[ (1 - \alpha - \beta \cdot \sigma) \left( \frac{1 + \mathbf{n}_2 \cdot \sigma}{2} \right) \right] \\ &= \eta_1 (\alpha + \mathbf{n}_1 \cdot \beta) + \eta_2 (1 - \alpha - \mathbf{n}_2 \cdot \beta) \\ &= \eta_2 + (\eta_1 - \eta_2) \alpha + (\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2) \cdot \beta. \end{aligned} \quad (3.3)$$

この  $p_o$  に対して Schwarz の不等式を用いると, 次のような不等式が得られる.

$$p_o \leq \eta_2 + (\eta_1 - \eta_2) \alpha + |\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2| |\beta|. \quad (3.4)$$

この不等式が  $p_o$  の上限を与える. それゆえ,  $p_o$  を最大にするためには, 次のような

$$A = (\eta_1 - \eta_2) \alpha + |\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2| |\beta|, \quad (3.5)$$

を最大にする  $\alpha, |\beta|$  を決定しなければならない. まず, (3.5) 式を  $\alpha$  について解くと,

$$\alpha = -\frac{|\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2|}{\eta_1 - \eta_2} |\beta| + \frac{A}{\eta_1 - \eta_2}, \quad (3.6)$$

となる. これは  $|\beta|$  と  $\alpha$  が張る平面上の直線を表す.

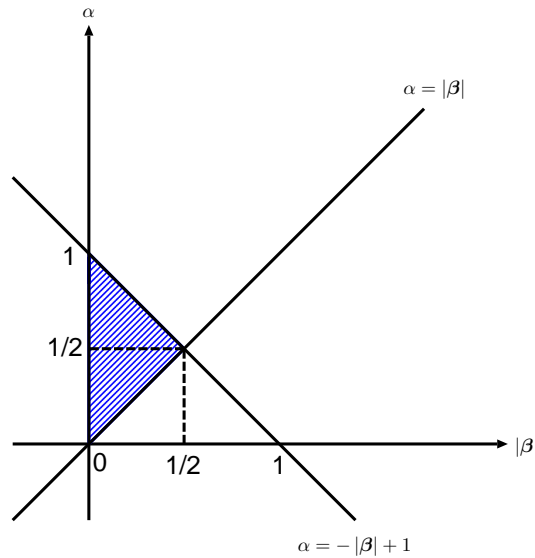


図 3.1: (3.7) 式を満たす  $|\beta|$  と  $\alpha$  の範囲

また, (3.1a) 式から,  $E_1, E_2$  それぞれの小さい方の固有値は正でなければならないことがわかる. それゆえ,  $\alpha$  は次のような不等式を満たさなければならない.

$$|\beta| \leq \alpha \leq -|\beta| + 1. \quad (3.7)$$

今, (3.7) 式を満たす  $|\beta|$  と  $\alpha$  の範囲は図 3.1 の斜線部である. この範囲で,  $A$  が最大となるのは (3.6) 式で与えられた直線が点  $(|\beta|, \alpha) = (1/2, 1/2)$  を通るときである.

したがって, 最大識別成功確率  $p_{\max}$  は次のように与えられる.

$$\begin{aligned} p_{\max} &= \eta_2 + \frac{\eta_1 - \eta_2}{2} + \frac{|\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2|}{2} \\ &= \frac{1}{2} \left[ 1 + \sqrt{1 - 2\eta_1 \eta_2 (1 + \mathbf{n}_1 \cdot \mathbf{n}_2)} \right]. \end{aligned}$$

Bloch ベクトル表示を元の量子状態  $|\phi_1\rangle, |\phi_2\rangle$  で書き直すと,

$$p_{\max} = \frac{1}{2} \left( 1 + \sqrt{1 - 4\eta_1 \eta_2 |\langle \phi_1 | \phi_2 \rangle|^2} \right), \quad (3.8)$$

となる. そして, この  $p_{\max}$  を実現する最適な POVM は次のように与えられる.

$$E_1 = \frac{1}{2} \left[ 1 + \frac{\eta_2 - \eta_1 + 2(\eta_1 |\phi_1\rangle\langle\phi_1| - \eta_2 |\phi_2\rangle\langle\phi_2|)}{\sqrt{1 - 4\eta_1 \eta_2 |\langle \phi_1 | \phi_2 \rangle|^2}} \right], \quad (3.9)$$

$$E_2 = I - E_1. \quad (3.10)$$

## 3.2 Unambiguous discrimination

Unambiguous discrimination では, 識別に間違いは許されない. その代わり, 識別が成功する可能性がない場合に”わからない”という推定を許容し, 識別成功確率を最大にする. そのとき, 測定は  $|\phi_1\rangle$  と  $|\phi_2\rangle$  によって張られる 2 次元部分空間上の POVM で記述され, 3 つの要素  $\{E_1, E_2, E_0\}$  から構成される. 要素  $E_1, E_2$  は測定結果 1 を得れば, 与えられた状態は  $\rho_1$  であると推定し, 測定結果 2 を得れば, 与えられた状態は  $\rho_2$  であると推定することにそれぞれ対応する. 要素  $E_0$  は”わからない”という推定に対応する. さらに,  $E_1, E_2, E_0$  は POVM 要素であることから, 次のような条件を満たす.

$$E_0 \geq 0, \quad E_1 \geq 0, \quad E_2 \geq 0, \quad (3.11a)$$

$$E_0 + E_1 + E_2 = I. \quad (3.11b)$$

識別成功確率  $p_o$  は次のように与えられる.

$$p_o = \eta_1 \text{tr}[E_1 \rho_1] + \eta_2 \text{tr}[E_2 \rho_2]. \quad (3.12)$$

Unambiguous discrimination の設定では, 識別に間違いは許されない. それゆえ, 与えられた状態が  $\rho_2$  であるとき, 測定結果 1 を得る条件付き確率  $P_{\rho_2|E_1}$  および与えられた状態が  $\rho_1$  であるとき, 測定結果 2 を得る条件付き確率  $P_{\rho_1|E_2}$  は 0 でなければならない.

$$P_{\rho_2|E_1} = \frac{P_{E_1, \rho_2}}{P_{E_1}} = \frac{P_{E_1, \rho_2}}{P_{E_1, \rho_1} + P_{E_1, \rho_2}} = \frac{\eta_2 \text{tr}[E_1 \rho_2]}{\eta_1 \text{tr}[E_1 \rho_1] + \eta_2 \text{tr}[E_1 \rho_2]} = 0, \quad (3.13a)$$

$$P_{\rho_1|E_2} = \frac{P_{E_2,\rho_1}}{P_{E_2}} = \frac{P_{E_2,\rho_1}}{P_{E_2,\rho_1} + P_{E_2,\rho_2}} = \frac{\eta_1 \text{tr}[E_2 \rho_1]}{\eta_1 \text{tr}[E_2 \rho_1] + \eta_2 \text{tr}[E_2 \rho_2]} = 0. \quad (3.13b)$$

今,  $|\phi_1\rangle$  と  $|\phi_2\rangle$  の張る 2 次元部分空間を考えているので, 状態  $\rho_i$  は Bloch ベクトルを用いて, 次のように表すことができる.

$$\rho_i = \frac{1 + \mathbf{n}_i \cdot \boldsymbol{\sigma}}{2} \quad (i = 1, 2).$$

さらに, POVM 要素  $E_1, E_2, E_0$  も 2 次元部分空間上の Hermite 演算子であるので, 次のように表すことができる.

$$\begin{aligned} E_1 &= \alpha_1 + \boldsymbol{\beta}_1 \cdot \boldsymbol{\sigma}, & E_2 &= \alpha_2 + \boldsymbol{\beta}_2 \cdot \boldsymbol{\sigma}, \\ E_0 &= I - (E_1 + E_2) = 1 - (\alpha_1 + \alpha_2) - (\boldsymbol{\beta}_1 + \boldsymbol{\beta}_2) \cdot \boldsymbol{\sigma}, \end{aligned}$$

ここで,  $\boldsymbol{\sigma}$  は Pauli 行列である.

したがって, 識別成功確率  $p_o$  は次のように書き換えられる.

$$\begin{aligned} p_o &= \eta_1 \text{tr} \left[ (\alpha_1 + \boldsymbol{\beta}_1 \cdot \boldsymbol{\sigma}) \left( \frac{1 + \mathbf{n}_1 \cdot \boldsymbol{\sigma}}{2} \right) \right] + \eta_2 \text{tr} \left[ (\alpha_2 + \boldsymbol{\beta}_2 \cdot \boldsymbol{\sigma}) \left( \frac{1 + \mathbf{n}_2 \cdot \boldsymbol{\sigma}}{2} \right) \right] \\ &= \eta_1 (\alpha_1 + \boldsymbol{\beta}_1 \cdot \mathbf{n}_1) + \eta_2 (\alpha_2 + \boldsymbol{\beta}_2 \cdot \mathbf{n}_2). \end{aligned} \quad (3.14)$$

そして, (3.13) 式から, 次のような関係が得られる.

$$\alpha_1 = -\boldsymbol{\beta}_1 \cdot \mathbf{n}_2, \quad \alpha_2 = -\boldsymbol{\beta}_2 \cdot \mathbf{n}_1.$$

この関係式に対して, それぞれ Schwarz の不等式を用いると,

$$\begin{aligned} \alpha_1 &= -\boldsymbol{\beta}_1 \cdot \mathbf{n}_2 = \boldsymbol{\beta}_1 \cdot (-\mathbf{n}_2) \leq |\boldsymbol{\beta}_1|, \\ \alpha_2 &= -\boldsymbol{\beta}_2 \cdot \mathbf{n}_1 = \boldsymbol{\beta}_2 \cdot (-\mathbf{n}_1) \leq |\boldsymbol{\beta}_2|, \end{aligned}$$

という不等式が得られる. 一方,  $E_1, E_2$  の半正定値性から, 小さい方の固有値はそれぞれ正でなければならない. それゆえ, 次のような関係が成り立つことは明らかである.

$$\alpha_1 = |\boldsymbol{\beta}_1|, \quad \alpha_2 = |\boldsymbol{\beta}_2|.$$

したがって, ベクトル  $\boldsymbol{\beta}_1, \boldsymbol{\beta}_2$  は次のように与えられる.

$$\boldsymbol{\beta}_1 = -\alpha_1 \mathbf{n}_2, \quad \boldsymbol{\beta}_2 = -\alpha_2 \mathbf{n}_1. \quad (3.15)$$

これは  $\boldsymbol{\beta}_1$  が  $\mathbf{n}_2$  と直交する向きにあり,  $\boldsymbol{\beta}_2$  が  $\mathbf{n}_1$  と直交する向きにあることを意味する. 以上から,  $p_o$  は次のように書き換えられる.

$$\begin{aligned} p_o &= \eta_1 [\alpha_1 + (-\alpha_1 \mathbf{n}_2) \cdot \mathbf{n}_1] + \eta_2 [\alpha_2 + (-\alpha_2 \mathbf{n}_1) \cdot \mathbf{n}_2] \\ &= (\eta_1 \alpha_1 + \eta_2 \alpha_2) (1 - \mathbf{n}_1 \cdot \mathbf{n}_2). \end{aligned} \quad (3.16)$$

この  $p_o$  を最大にするためには, 次のような

$$A' = \eta_1 \alpha_1 + \eta_2 \alpha_2, \quad (3.17)$$



を最大にする  $\alpha_1, \alpha_2$  を決定しなければならない。まず, (3.17) 式を  $\alpha_2$  について解くと,

$$\alpha_2 = -\frac{\eta_1}{\eta_2}\alpha_1 + \frac{A'}{\eta_2}, \quad (3.18)$$

となる。これは  $\alpha_1$  と  $\alpha_2$  が張る平面上の直線を表す。さらに,  $E_0$  が半正定値演算子であることから, 小さい方の固有値は正でなければならない。それゆえ, 次のような不等式が得られる。

$$\alpha_2 \geq \frac{2\alpha_1 - 1}{2[(1 - \mathbf{n}_1 \cdot \mathbf{n}_2)\alpha_1 - 1]}, \quad (3.19)$$

ただし,  $\alpha_2$  は次のような不等式を満たさなければならないことに注意する。

$$\alpha_2 \leq 1 - \alpha_1. \quad (3.20)$$

今, (3.19), (3.20) 式を満たす  $\alpha_1$  と  $\alpha_2$  の範囲は図 3.2 の斜線部である。この範囲で,  $A'$  が最大となるのは (3.18) 式で与えられた直線の傾きが (3.19) 式で与えられた双曲線の傾きと一致するときである。

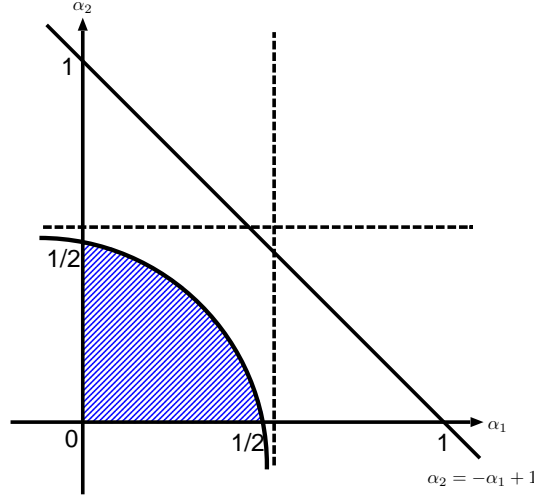


図 3.2: (3.19), (3.20) 式を満たす  $\alpha_1$  と  $\alpha_2$  の範囲

まず, 双曲線の傾きを求めるために, 次のような  $\alpha_1$  の関数  $f(\alpha_1)$  を定義する。

$$f(\alpha_1) = \frac{2\alpha_1 - 1}{2[(1 - \mathbf{n}_1 \cdot \mathbf{n}_2)\alpha_1 - 1]}.$$

この  $f(\alpha_1)$  を  $\alpha_1$  に関して微分すると, 次のような傾きが得られる。

$$\frac{df(\alpha_1)}{d\alpha_1} = - \left( \frac{1 + \mathbf{n}_1 \cdot \mathbf{n}_2}{2[(1 - \mathbf{n}_1 \cdot \mathbf{n}_2)\alpha_1 - 1]} \right)^2$$

この傾きが (3.20) 式で与えられた直線の傾きと一致することから,  $\alpha_1$  は次のように与えられる。

$$\alpha_1 = \frac{1}{1 - \mathbf{n}_1 \cdot \mathbf{n}_2} \left[ 1 \pm \sqrt{\frac{\eta_2}{\eta_1} \left( \frac{1 + \mathbf{n}_1 \cdot \mathbf{n}_2}{2} \right)} \right]. \quad (3.21)$$

今,  $\alpha_1$  の許される範囲は  $0 \leq \alpha_1 \leq 1/2$  である. これを満たすためには,  $\alpha_1$  は負の符号をとらなければならない. それゆえ, これ以降は  $\alpha_1$  の複号に関して, 負の符号をとる. さらに,  $\alpha_2$  も次のように与えられる.

$$\alpha_2 = \frac{1}{1 - \mathbf{n}_1 \cdot \mathbf{n}_2} \left[ 1 - \sqrt{\frac{\eta_1}{\eta_2} \left( \frac{1 + \mathbf{n}_1 \cdot \mathbf{n}_2}{2} \right)} \right]. \quad (3.22)$$

したがって, 最大識別成功確率  $p_{\max}$  は次のように与えられる.

$$p_{\max} = 1 - 2\sqrt{\eta_1 \eta_2 \left( \frac{1 + \mathbf{n}_1 \cdot \mathbf{n}_2}{2} \right)}.$$

Bloch ベクトル表示を元の量子状態  $|\phi_1\rangle, |\phi_2\rangle$  で書き直すと,

$$p_{\max} = 1 - 2\sqrt{\eta_1 \eta_2} |\langle \phi_1 | \phi_2 \rangle|, \quad (3.23)$$

となる.

最後に, 図 3.2 から見てわかるように, 最適な  $\alpha_1, \alpha_2$  の許される範囲はそれぞれ  $0 \leq \alpha_1 \leq 1/2, 0 \leq \alpha_2 \leq 1/2$  であった. これは生起確率によって場合分けされることを意味する. したがって, それぞれの場合について,  $P_{\max}, \alpha_1, \alpha_2$  は次のように与えられる.

$$(i) \quad \sqrt{\frac{\eta_2}{\eta_1}} < |\langle \phi_1 | \phi_2 \rangle| \quad \text{のとき}$$

$$p_{\max} = \eta_1 (1 - |\langle \phi_1 | \phi_2 \rangle|^2). \quad (3.24)$$

$$\alpha_1 = \frac{1}{2}, \quad (3.25a)$$

$$\alpha_2 = 0. \quad (3.25b)$$

$$(ii) \quad |\langle \phi_1 | \phi_2 \rangle| \leq \sqrt{\frac{\eta_2}{\eta_1}} \leq \frac{1}{|\langle \phi_1 | \phi_2 \rangle|} \quad \text{のとき}$$

$$p_{\max} = 1 - 2\sqrt{\eta_1 \eta_2} |\langle \phi_1 | \phi_2 \rangle|. \quad (3.26)$$

$$\alpha_1 = \frac{1}{2(1 - |\langle \phi_1 | \phi_2 \rangle|^2)} \left( 1 - \sqrt{\frac{\eta_2}{\eta_1}} |\langle \phi_1 | \phi_2 \rangle| \right), \quad (3.27a)$$

$$\alpha_2 = \frac{1}{2(1 - |\langle \phi_1 | \phi_2 \rangle|^2)} \left( 1 - \sqrt{\frac{\eta_1}{\eta_2}} |\langle \phi_1 | \phi_2 \rangle| \right). \quad (3.27b)$$

$$(iii) \quad \frac{1}{|\langle \phi_1 | \phi_2 \rangle|} < \sqrt{\frac{\eta_2}{\eta_1}} \quad \text{のとき}$$

$$p_{\max} = \eta_2 (1 - |\langle \phi_1 | \phi_2 \rangle|^2). \quad (3.28)$$

$$\alpha_1 = 0, \quad (3.29a)$$

$$\alpha_2 = \frac{1}{2}. \quad (3.29b)$$

## 第4章 2つの純粋状態のエラーマージン のある識別問題

識別間違い確率に対してエラーマージンを課すことで, minimum-error discrimination の設定と unambiguous discrimination の設定を統一的に扱う識別問題を考察し, 一般の生起確率を持つ2つの純粋状態の場合について分析する. 最適な測定は3つのタイプに分類され, 測定の3つのタイプの1つがパラメータ (生起確率とエラーマージン) に依存して最適となる. パラメータ空間での3つの領域を決定し, それぞれの領域での最大識別成功確率を完全に解析的な形式で求める. また, 識別間違い確率に対するエラーマージンの課し方には2つのタイプが考えられる. この2つのタイプのそれぞれの最大識別成功確率の間にある関係を示す.

### 4.1 問題の定式化と解

それぞれ生起確率  $\eta_i$  の2つの純粋状態  $\rho_i = |\phi_i\rangle\langle\phi_i|$  ( $i = 1, 2$ ) の識別問題を考察する. 自明で特別な場合を除いて,  $\eta_i \neq 0$  を仮定する. 2つの状態は線形独立であることも仮定し, それら2つの状態によって張られた2次元部分空間  $V$  を考える. 測定は空間  $V$  上の POVM によって記述され, それは3つの要素  $\{E_\mu\}_{\mu=1}^3$  から成り立つ.  $\mu = 1$  or  $2$  によって分類される測定結果は与えられた状態が  $\rho_\mu$  であると推定することを意味する. 要素  $E_3$  は”わからない”という推定を示す.

識別成功確率  $p_o$  と平均間違い確率  $p_\times$  は次のように与えられる.

$$p_o \equiv P_{\rho_1, E_1} + P_{\rho_2, E_2} = \eta_1 \text{tr}[E_1 \rho_1] + \eta_2 \text{tr}[E_2 \rho_2], \quad (4.1)$$

$$p_\times \equiv P_{\rho_1, E_2} + P_{\rho_2, E_1} = \eta_1 \text{tr}[E_2 \rho_1] + \eta_2 \text{tr}[E_1 \rho_2]. \quad (4.2)$$

この設定では, 平均間違い確率  $p_\times$  がエラーマージン  $m$  ( $0 \leq m \leq 1$ ) を越えてはならないことを要請する. そして, 課題は次のような条件の下で識別成功確率  $p_o$  を最大にすることである.

$$E_1 \geq 0, E_2 \geq 0, E_3 \geq 0, \quad (4.3a)$$

$$E_1 + E_2 + E_3 = I, \quad (4.3b)$$

$$p_\times \leq m, \quad (4.3c)$$

ここで, (4.3a), (4.3b) 式は POVM に関するいつもの条件である.

この問題は semidefinite programming(SDP) の1つとして定式化できる [37–39]. SDP の一般定理によると, 最適な POVM に対する必要十分条件を書くことができる. 我々の目的に対して, それらが十分条件であることを見るためには十分である.

一方, 次のような条件を満たす空間  $V$  上に作用する Hermite 演算子  $Y$ , 実数  $y$  が存在するとする.

$$Y \geq 0, \quad (4.4a)$$

$$Y \geq \eta_1 \rho_1 - y \eta_2 \rho_2, \quad (4.4b)$$

$$Y \geq \eta_2 \rho_2 - y \eta_1 \rho_1, \quad (4.4c)$$

$$y \geq 0. \quad (4.4d)$$

このとき, 次のように定義された

$$d \equiv \text{tr}[Y] + my, \quad (4.5)$$

が識別成功確率  $p_o$  に対して上限を与える. そして, それは次のように証明できる.

$$\begin{aligned} p_o &= \text{tr}[E_1 \eta_1 \rho_1] + \text{tr}[E_2 \eta_2 \rho_2] \\ &\leq \text{tr}[E_1 (Y + y \eta_2 \rho_2)] + \text{tr}[E_2 (Y + y \eta_1 \rho_1)] \\ &= \text{tr}[(E_1 + E_2) Y] + y p_{\times} \\ &\leq \text{tr}[Y] + ym = d. \end{aligned}$$

さらに, この上限が次のような関係が成立する場合に限り, 達成されることは明らかである.

$$E_1 [Y - (\eta_1 \rho_1 - y \eta_2 \rho_2)] = 0, \quad (4.6a)$$

$$E_2 [Y - (\eta_2 \rho_2 - y \eta_1 \rho_1)] = 0, \quad (4.6b)$$

$$E_3 Y = 0, \quad (4.6c)$$

$$y(m - p_{\times}) = 0. \quad (4.6d)$$

したがって, (4.3), (4.4), (4.6) 式によって与えられた条件式は最適な解に対する十分条件である. これから見ていくように, 任意のパラメータ  $\eta_i, m, \langle \phi_1 | \phi_2 \rangle$  に対して, この条件を満たす解を構築することができる. SDP の一般定理はそれが必要条件でもあることを示す [37–39]. 条件式 (4.4) の下で  $d$  を最小化することは双対問題と呼ばれる. 一方, 最初の問題である条件式 (4.3) の下で  $p_o$  を最大化することは主問題と呼ばれる.

初めに, 2次元空間  $V$  上の演算子である最適な POVM 要素のランクを見てみよう. ただし, それらが最大でもランクが 1 であることに注意しなければならない. それは次のような方法で見ることができる. まず, POVM 要素  $E_3$  のランクが 2 であるとする. 条件式 (4.6c) は  $Y = 0$  であることを要請する. そして, (4.4b), (4.4c) 式から次のような関係が成り立つ.

$$\begin{aligned} y\eta_2\rho_2 &\geq \eta_1\rho_1, \\ y\eta_1\rho_1 &\geq \eta_2\rho_2. \end{aligned}$$

それぞれ状態  $|\phi_i\rangle$  に直交する状態  $|\phi_i^\perp\rangle$  ( $i = 1, 2$ ) を定義し, これらの 2 つの不等式に対して, それぞれ状態  $|\phi_i^\perp\rangle$  を作用させると, 次のような関係が得られる.

$$\begin{aligned} 0 &\geq \eta_1 |\langle \phi_2^\perp | \phi_1 \rangle|^2, \\ 0 &\geq \eta_2 |\langle \phi_1^\perp | \phi_2 \rangle|^2. \end{aligned}$$

今,  $\eta_i > 0$  であることから, これらの不等式は状態  $|\phi_1\rangle$  と状態  $|\phi_2\rangle$  がグローバル位相因子を除けば, 同一であることを意味する. これは  $|\phi_1\rangle$  と  $|\phi_2\rangle$  の線形独立性に矛盾する. 次に, POVM 要素  $E_1$  のランクが 2 であるとする. (4.6a) 式から,  $Y = \eta_1\rho_1 - y\eta_2\rho_2$  が得られる. そのとき, (4.4a), (4.4c) 式は次のような不等式が成り立つことを要請する.

$$\begin{aligned} \eta_1\rho_1 &\geq y\eta_2\rho_2, \\ \eta_1\rho_1 &\geq \eta_2\rho_2. \end{aligned}$$

これは先ほどと同様の議論から,  $\eta_2 \neq 0$  という仮定と状態  $|\phi_1\rangle$  と状態  $|\phi_2\rangle$  の線形独立性に矛盾する. また,  $E_2$  のランクが 2 であるとした場合についても, 同様の議論がなされる. したがって, 最適な POVM 要素のランクは最大でも 1 であることが示された.

第 4 章の最初でも述べたように, 3 つの測定のタイプがあり, それらの 1 つが生起確率とエラーマージンのパラメータ空間の領域に依存して最適になる. この分類は POVM のランクによってなされる. Minimum-error 領域では, 最適な POVM は minimum-error discrimination のそれである. そして, それは  $E_3 = 0$  であると同時に,  $E_1, E_2$  のランクは 1 であることを意味する. Single-state 領域では, 最適な測定は 2 つの状態のうち 1 つを無視して 2 つの結果だけを生み出す. この場合,  $E_1$  か  $E_2$  のどちらかは 0 であり, 残りの 2 つの POVM 要素のランクは 1 である. Intermediate 領域はすべての POVM 要素のランクが 1 であり, 3 つの結果を得る確率は 0 ではない.

以下では, まず, 主な結果を述べ, それらの導出は後の節で詳しく説明する. 一般性の損失なしに  $\eta_1 \leq \eta_2$  を仮定する. 式をより簡単にするために, 次のような  $S, T$  を定義する.

$$S \equiv |\langle \phi_1 | \phi_2 \rangle|^2, \quad (4.7)$$

$$T \equiv 1 - |\langle \phi_1 | \phi_2 \rangle|^2. \quad (4.8)$$

パラメータ空間は次のような 3 つの領域に分類される.

$$\begin{aligned} m_c &\leq m \leq 1 && (\text{minimum-error 領域}), \\ m'_c &\leq m \leq m_c && (\text{intermediate 領域}), \\ 0 &\leq m \leq m'_c && (\text{single-state 領域}), \end{aligned}$$

ここで, 2 つの境界エラーマージン  $m_c, m'_c$  は次のように定義される.

$$m_c \equiv \frac{1}{2} \left( 1 - \sqrt{1 - 4\eta_1\eta_2 S} \right), \quad (4.9)$$

$$m'_c \equiv \begin{cases} \frac{(\eta_1 - \sqrt{\eta_1\eta_2 S})^2}{1 - 2\sqrt{\eta_1\eta_2 S}} & (\eta_1 \leq \eta_2 S), \\ 0 & (\eta_1 \geq \eta_2 S). \end{cases} \quad (4.10)$$

図 4.1 は  $\sqrt{S} = |\langle \phi_1 | \phi_2 \rangle| = 0.9$  の場合のパラメータ空間での 3 つの領域を図示した.

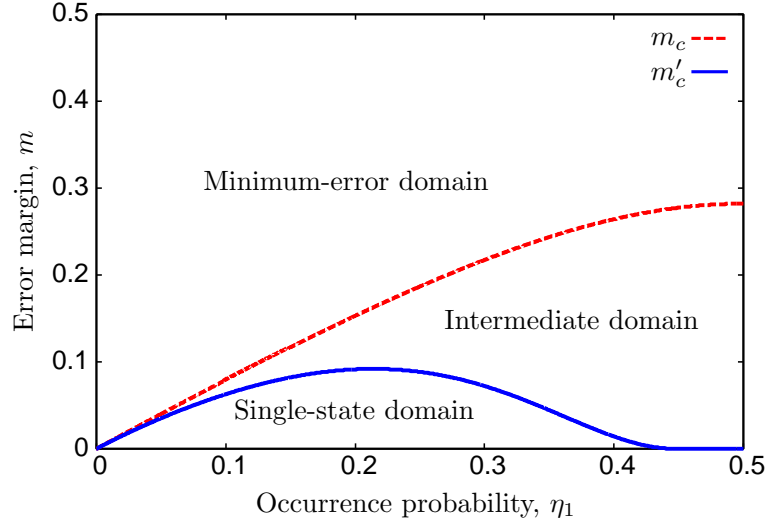


図 4.1: 生起確率  $\eta_1$  とエラーマージン  $m$  のパラメータ空間での 3 つの領域.

それぞれの領域での最大識別成功確率は次のように与えられる.

$$p_{\max} = \begin{cases} \frac{1}{2} (1 + \sqrt{1 - 4\eta_1\eta_2 S}) & (m_c \leq m \leq 1), \\ \left( \sqrt{m} + \sqrt{1 - 2\sqrt{\eta_1\eta_2 S}} \right)^2 & (m'_c \leq m \leq m_c), \\ \eta_2 \left( \sqrt{\frac{m}{\eta_1} S} + \sqrt{\frac{\eta_1 - m}{\eta_1} T} \right)^2 & (0 \leq m \leq m'_c). \end{cases} \quad (4.11)$$

$m_c$  は実は最適な minimum-error discrimination の平均間違い確率である. もし,  $m_c \leq m$  ならば, 識別間違い確率に対する制限は作用しない. これが minimum-error 領域の  $p_{\max}$  が minimum-error discrimination のそれによって与えられる理由である. 図 4.2 では, 生起確率  $\eta_1 = 0.3$  と固定して, エラーマージン  $m$  に対して最大識別成功確率  $p_{\max}$  と  $\text{tr}[E_1]$  をプロットした.  $\text{tr}[E_1]$  のプロットは single-state 領域と intermediate 領域との間の境界を明らかに示すが,  $p_{\max}$  のカーブは  $m = m'_c$  で滑らかである.

Unambiguous discrimination ( $m = 0$ ) では, 十分に小さい  $\eta_1$  に関して, 最適な測定は常に single-state 領域のそれである. これは直観的に無理なく現れる. しかしながら, 図 4.1 は有限のエラーマージンに対してはそれが真実ではないことを示す. 例えば, エラーマージンを  $m = 0.06$  付近に固定し, 生起確率  $\eta_1$  を 0.5 から 0 まで変化させる. そのとき, 最適な測定のタイプは intermediate 領域から single-state 領域, intermediate 領域, そして, minimum-error 領域へと自明でない方法で変化する. そして, 図 4.3 は最大識別成功確率の 3 次元概観を図示した.

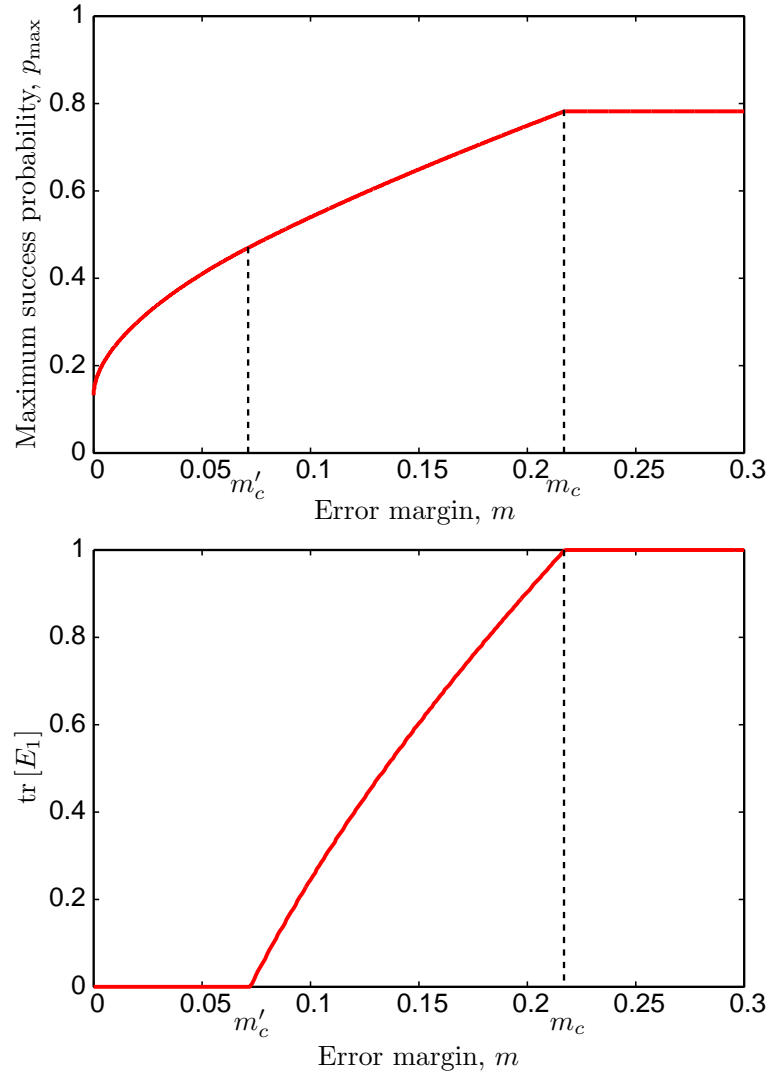


図 4.2: エラーマージン  $m$  に対する最大識別成功確率  $p_{\max}$  (上部) と  $\text{tr}[E_1]$  (下部).

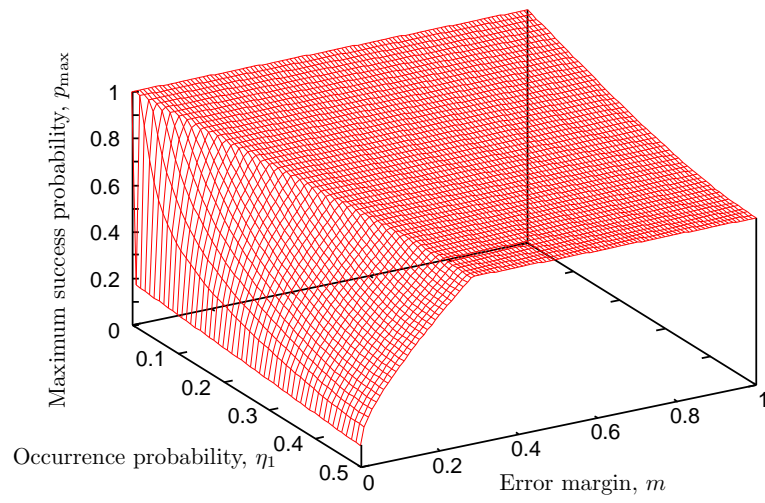


図 4.3: 生起確率  $\eta_1$  とエラーマージン  $m$  に対する最大識別成功確率  $p_{\max}$ .

## 4.2 Intermediate 領域

Intermediate 領域では, すべての POVM 要素  $E_1, E_2, E_3$  はゼロではなく, ランクは 1 である解を構成する. (4.6a), (4.6b), (4.6c) 式によって与えられた条件は次のように定義された半正定値演算子

$$\begin{aligned} Y_1 &\equiv Y - (\eta_1 \rho_1 - y \eta_2 \rho_2), \\ Y_2 &\equiv Y - (\eta_2 \rho_2 - y \eta_1 \rho_1), \end{aligned}$$

と演算子  $Y$  のランクが 1 であることを意味する. 状態  $\rho_i$  や空間  $V$  上で作用するその他の演算子に対して, Bloch ベクトル表示を用いると便利である.

$$\rho_i = \frac{1 + \mathbf{n}_i \cdot \boldsymbol{\sigma}}{2} \quad (i = 1, 2),$$

ここで,  $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$  は Pauli 行列である. さらに, 演算子  $Y$  は  $2 \times 2$  Hermite 演算子であることから, 次のように表すことができる.

$$Y = \alpha + \boldsymbol{\beta} \cdot \boldsymbol{\sigma}.$$

したがって, 演算子  $Y_1, Y_2$  は次のように書き換えることができる.

$$\begin{aligned} Y_1 &= \alpha - \frac{\eta_1 - y \eta_2}{2} + \left( \boldsymbol{\beta} - \frac{1}{2} \mathbf{a}_1 \right) \cdot \boldsymbol{\sigma}, \\ Y_2 &= \alpha - \frac{\eta_2 - y \eta_1}{2} + \left( \boldsymbol{\beta} - \frac{1}{2} \mathbf{a}_2 \right) \cdot \boldsymbol{\sigma}, \end{aligned}$$

ここで, 次のように定義された 2 つのベクトル  $\mathbf{a}_1, \mathbf{a}_2$  を導入した.

$$\mathbf{a}_1 \equiv \eta_1 \mathbf{n}_1 - y \eta_2 \mathbf{n}_2, \quad (4.12)$$

$$\mathbf{a}_2 \equiv \eta_2 \mathbf{n}_2 - y \eta_1 \mathbf{n}_1. \quad (4.13)$$

演算子  $Y_1, Y_2, Y$  のランクは 1 である, つまり, それぞれの小さい方の固有値はすべて 0 であるから, 次のような  $\alpha$  と  $\beta$  に関する 3 つの方程式を得る.

$$\alpha - \frac{\eta_1 - y \eta_2}{2} = \left| \boldsymbol{\beta} - \frac{1}{2} \mathbf{a}_1 \right|, \quad (4.14a)$$

$$\alpha - \frac{\eta_2 - y \eta_1}{2} = \left| \boldsymbol{\beta} - \frac{1}{2} \mathbf{a}_2 \right|, \quad (4.14b)$$

$$\alpha = |\boldsymbol{\beta}|. \quad (4.14c)$$

(4.14) 式から次のようなベクトル  $\boldsymbol{\beta}$  に関する 2 つの方程式が得られる.

$$\mathbf{a}_1 \cdot \boldsymbol{\beta} - (\eta_1 - y \eta_2) |\boldsymbol{\beta}| = y \eta_1 \eta_2 T,$$

$$\mathbf{a}_2 \cdot \boldsymbol{\beta} - (\eta_2 - y \eta_1) |\boldsymbol{\beta}| = y \eta_1 \eta_2 T.$$



これら 2 つの方程式の和と差はそれぞれ

$$|\beta| - (\eta_1 \mathbf{n}_1 + \eta_2 \mathbf{n}_2) \cdot \beta = \frac{2y\eta_1\eta_2 T}{y-1}, \quad (4.15)$$

$$(\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2) \cdot \beta - (\eta_1 - \eta_2) |\beta| = 0, \quad (4.16)$$

である. (4.15), (4.16) 式から, 次のような関係が得られる.

$$(\mathbf{n}_1 - \mathbf{n}_2) \cdot \beta = \frac{y(\eta_1 - \eta_2) T}{y-1}. \quad (4.17)$$

今, ベクトル  $\beta$  は Bloch ベクトル  $\mathbf{n}_1, \mathbf{n}_2$  が張る平面上にあることから, 次のように展開することができる.

$$\beta = u \frac{\mathbf{n}_1 + \mathbf{n}_2}{2} + v \frac{\mathbf{n}_1 - \mathbf{n}_2}{2}. \quad (4.18)$$

(4.17), (4.18) 式から, 係数  $v$  は次のように与えられる.

$$v = \frac{y}{2(y-1)} (\eta_1 - \eta_2). \quad (4.19)$$

また, (4.16), (4.18), (4.19) 式から, 次のような係数  $u$  に関する二次方程式が得られる.

$$u^2 - \frac{y}{y-1} u + \frac{y^2}{4(y-1)^2} \left( 1 - \frac{4\eta_1\eta_2}{S} \right) = 0.$$

$y \geq 1$  を満たさなければならないことに注意すると, 係数  $u$  は次のように与えられる.

$$u = \frac{y}{2(y-1)} \pm \frac{y}{y-1} \sqrt{\frac{\eta_1\eta_2}{S}}. \quad (4.20)$$

以上から, ベクトル  $\beta$  は次のように得られる.

$$\beta = \frac{y}{2(y-1)} \left\{ \left( \eta_1 \pm \sqrt{\frac{\eta_1\eta_2}{S}} \right) \mathbf{n}_1 + \left( \eta_2 \pm \sqrt{\frac{\eta_1\eta_2}{S}} \right) \mathbf{n}_2 \right\}. \quad (4.21)$$

そして,  $\alpha$  も次のように得られる.

$$\alpha = |\beta| = \frac{y}{2(y-1)} \left( 1 \pm 2\sqrt{\eta_1\eta_2 S} \right). \quad (4.22)$$

(4.4) 式を満たす  $Y$  と  $y$  が得られたので,  $d = \text{tr}[Y] + ym$  を計算することで, 識別成功確率に対する上限は次のように得られる.

$$d = \text{tr}[Y] + ym = \frac{y}{y-1} \left( 1 \pm 2\sqrt{\eta_1\eta_2 S} \right) + my. \quad (4.23)$$

上限  $d$  が最小化されるようにパラメータ  $y$  は決定される. そして, それは (4.23) 式を  $y$  について微分することで与えられる  $y$  に関する 2 次方程式

$$\frac{\partial}{\partial y} d = m - \frac{1 \pm 2\sqrt{\eta_1\eta_2 S}}{(y-1)^2} = 0,$$

を解くことで得られる.  $y \geq 1$  を満たさなければならないことに注意すれば, 得られた解のうちの1つが適することは明らかである. したがって,  $y$  は次のように与えられる.

$$y = 1 + \frac{\sqrt{1 \pm 2\sqrt{\eta_1 \eta_2 S}}}{\sqrt{m}}. \quad (4.24)$$

また, (4.23) 式は次のように書き換えられる.

$$d = \left(1 + \frac{1}{y-1}\right) \left(1 \pm 2\sqrt{\eta_1 \eta_2 S}\right) + m(y-1) + m.$$

この上限  $d$  に対して, 相加相乗平均の不等式を用いると, 次のような関係が得られる.

$$\begin{aligned} d &\geq 1 \pm 2\sqrt{\eta_1 \eta_2 S} + 2\sqrt{\left(1 \pm 2\sqrt{\eta_1 \eta_2 S}\right)m + m} \\ &= \left(\sqrt{m} + \sqrt{1 \pm 2\sqrt{\eta_1 \eta_2 S}}\right)^2. \end{aligned}$$

上限  $d$  は最小化されているので, この不等式は等号が成立する. したがって,  $d$  は次のように与えられる.

$$d = \left(\sqrt{m} + \sqrt{1 \pm 2\sqrt{\eta_1 \eta_2 S}}\right)^2. \quad (4.25)$$

$d, y$  の複号に関して, より小さい上限を得るために負の符号をとる. それに対応して, これ以後は (4.21), (4.22) 式の複号でも負の符号をとる.

(4.6a), (4.6b), (4.6c) 式によって与えられた条件は POVM 要素  $E_1, E_2, E_3$  が次のような形をとることを要求する.

$$E_\mu = \gamma_\mu (|\beta_\mu| - \beta_\mu \cdot \sigma) \quad (\mu = 1, 2, 3),$$

ここで, 次のようなベクトル  $\beta_\mu$  を定義した.

$$\beta_1 \equiv \beta - \frac{1}{2}\mathbf{a}_1, \quad \beta_2 \equiv \beta - \frac{1}{2}\mathbf{a}_2, \quad \beta_3 \equiv \beta.$$

問題は集合  $\{E_1, E_2, E_3\}$  が (4.3b) 式で与えられた POVM の完全性関係を尊重するように正の定数  $\gamma_1, \gamma_2, \gamma_3$  を選択することができるかどうかである. これは次のような3つのベクトル  $\beta_1, \beta_2, \beta_3$  に関して正の係数を持つ線形関係が存在する場合に限り, 可能である.

$$c_1\beta_1 + c_2\beta_2 + c_3\beta_3 = 0 \quad (c_1, c_2, c_3 \geq 0).$$

もし, このような線形関係が存在するならば, 係数  $\gamma_\mu$  は  $\sum_\mu \gamma_\mu |\beta_\mu| = 1$  であるように決定され, 全体が正の因子  $\gamma$  を持つ  $\gamma_\mu = \gamma c_\mu$  として構成できる.

3つのベクトルのそれぞれは2つの Bloch ベクトル  $\mathbf{n}_1, \mathbf{n}_2$  によって表すことができるので, すべての因子までが一意的であり, 次のような係数を持つ線形関係がまっすぐ

に見つけられる.

$$\begin{aligned} c_1 &= \frac{y}{y+1} \left( \sqrt{m} - \frac{\sqrt{\eta_1 \eta_2 S} - \eta_1}{\sqrt{1 - 2\sqrt{\eta_1 \eta_2 S}}} \right), \\ c_2 &= \frac{y}{y+1} \left( \sqrt{m} - \frac{\sqrt{\eta_1 \eta_2 S} - \eta_2}{\sqrt{1 - 2\sqrt{\eta_1 \eta_2 S}}} \right), \\ c_3 &= \sqrt{\frac{\eta_1 \eta_2 S}{m}} - \sqrt{m} - \sqrt{1 - 2\sqrt{\eta_1 \eta_2 S}}. \end{aligned}$$

$c_\mu$  の符号は  $\eta_1, \eta_2, S, m$  に依存して変化する. ここで,  $\eta_1 \leq \eta_2$  と想定しているので,  $c_2$  は常に正である. さらに,  $m \geq m'_c$  ならば,  $c_1$  は正であることと  $m \leq m_c$  ならば,  $c_3$  は正であることがわかる. ここで,  $m_c, m'_c$  は (4.9), (4.10) 式でそれぞれ定義されている. したがって, エラーマージン  $m$  が  $m'_c \leq m \leq m_c$  の範囲にあれば, 集合  $\{E_1, E_2, E_3\}$  は POVM である.

残りの条件は (4.3c), (4.6d) 式である. そして, それらは  $y \geq 1$  なので,  $p_\times = m$  と変形することができる.  $p_\times = m$  という関係が成立することは上で構成した POVM を用いて計算することで証明できる. これは偶然の一致ではなく, パラメータ  $y$  をどのように決定したかの結果である. パラメータ  $y$  は (4.23) 式によって与えられた上限  $d$  が最小となるように決定された. すなわち, 次のようなパラメータ  $y$  に関する偏微分方程式の解である.

$$\frac{\partial}{\partial y} d = \frac{\partial}{\partial y} \text{tr}[Y] + m = 0.$$

さらに,  $\frac{\partial}{\partial y} \text{tr}[Y] = -p_\times$  を示すことができる. そして, それは  $d$  の最小化が  $p_\times = m$  という関係を導くことを意味する. これは次のような方法で見ることができる. 2つの半正定値演算子  $A(y), B(y)$  が変数  $y$  に依存し,  $A(y)B(y) = 0$  を満たすとする. そのとき,  $\text{tr}[A(y)B'(y)] = 0$  を示すことができる. これを証明するために, 次のような関数  $f(x)$  を定義する.

$$f(x) \equiv \text{tr}[A(y)B(y+x)].$$

任意の  $x$  に関して  $f(x) \geq 0$  ならば,  $f(0) = 0$  であることに注目する. そして, それは関数  $f(x)$  が  $x = 0$  で最小値を持つことを意味する.  $f'(0) = 0$  であることから, 示したい結果は直ちに示される. 今, 演算子  $Y_1, Y_2, Y$  と POVM 要素  $E_\mu$  はすべて半正定値であり,  $E_1 Y_1 = E_2 Y_2 = E_3 Y = 0$  を満たす. それゆえ, 次のような関係を得る.

$$\begin{aligned} \frac{\partial}{\partial y} \text{tr}[Y] &= \text{tr} \left[ E_1 \frac{\partial Y}{\partial y} \right] + \text{tr} \left[ E_2 \frac{\partial Y}{\partial y} \right] + \text{tr} \left[ E_3 \frac{\partial Y}{\partial y} \right] \\ &= \text{tr} \left[ E_1 \frac{\partial Y_1}{\partial y} \right] + \text{tr} \left[ E_2 \frac{\partial Y_2}{\partial y} \right] + \text{tr} \left[ E_3 \frac{\partial Y}{\partial y} \right] - p_\times \\ &= -p_\times. \end{aligned}$$

したがって, もし, エラーマージン  $m$  が  $m'_c \leq m \leq m_c$  の範囲にあるならば, (4.25) 式の上限は達成され, 最大識別成功確率  $p_{\max}$  は次のように与えられる.

$$p_{\max} = \left( \sqrt{m} + \sqrt{1 - 2\sqrt{\eta_1 \eta_2 S}} \right)^2. \quad (4.26)$$

最適な POVM を用いて, 次のような対称性が成立することがわかった.

$$P_{\rho_2|E_1} = P_{\rho_1|E_2}, \quad (4.27)$$

$$P_{\rho_1|E_3} = P_{\rho_2|E_3}, \quad (4.28)$$

ここで, 次のように定義される条件付き確率を導入した.

$$P_{\rho_i|E_\mu} \equiv \frac{P_{\rho_i, E_\mu}}{P_{E_\mu}}, \quad P_{E_\mu} \equiv P_{\rho_1, E_\mu} + P_{\rho_2, E_\mu}.$$

問題では一般の生起確率を持つ  $\rho_1$  と  $\rho_2$  との間には明らかな対称性がないので, これは注目すべきことである. (4.27) 式によって与えられた 2 つの条件付き間違い確率の対称性は 4.4 節で重要になる.

この節を終える前に, それらの対称性がどのようにして現れたのかを明らかにするために簡単な議論を述べる. 次のような 2 つのベクトル  $C, X$  を定義する.

$$\begin{aligned} C &\equiv \left( \sqrt{P_{\rho_1, E_1}}, \sqrt{P_{\rho_2, E_2}} \right), \\ X &\equiv \left( \sqrt{P_{\rho_2, E_1}}, \sqrt{P_{\rho_1, E_2}} \right). \end{aligned}$$

そのとき, 識別成功確率  $p_o$  は  $|C|^2$  によって与えられる. また, 三角不等式を用いると, 次のような関係が成立することが言える.

$$\sqrt{p_o} = |C| \leq |X| + |C - X|. \quad (4.29)$$

今,  $|X| = \sqrt{p_{\times}}$  であることに注目する. そして, それは  $\sqrt{m}$  を越えてはならない.  $|C - X|$  の上限は次のような方法で決定することができる.

$$\begin{aligned} |C - X|^2 &= C^2 + X^2 - 2C \cdot X \\ &= 1 - P_{\rho_1, E_3} - P_{\rho_2, E_3} - 2C \cdot X \\ &\leq 1 - 2 \left( \sqrt{P_{\rho_1, E_3} P_{\rho_2, E_3}} + C \cdot X \right) \\ &= 1 - 2\sqrt{\eta_1 \eta_2} \sum_{\mu=1}^3 \sqrt{q_{\mu}^{(1)} q_{\mu}^{(2)}}, \end{aligned}$$

ここで, 次のような相加相乗平均の不等式を用いた.

$$P_{\rho_1, E_3} + P_{\rho_2, E_3} \geq 2\sqrt{P_{\rho_1, E_3} P_{\rho_2, E_3}}, \quad (4.30)$$

さらに, 次のような 2 つの確率分布  $q_{\mu}^{(1)}, q_{\mu}^{(2)}$  を定義した.

$$q_{\mu}^{(i)} \equiv \text{tr} [\rho_i E_{\mu}] \quad (i = 1, 2, \mu = 1, 2, 3).$$

$\sum_{\mu=1}^3 \sqrt{q_{\mu}^{(1)} q_{\mu}^{(2)}}$  という表現は 2 つの状態  $\rho_1, \rho_2$  に関して測定結果  $\mu$  を得る 2 つの古典的確率分布  $q_{\mu}^{(1)}, q_{\mu}^{(2)}$  の忠実度である. この古典的忠実度は 2 つの状態の量子的忠実度

$|\langle \phi_1 | \phi_2 \rangle| = \sqrt{S}$  によって制限され、より低くなることが知られている [41]. したがって、次のような  $p_o$  に対する上限を得る.

$$p_o \leq \left( \sqrt{m} + \sqrt{1 - 2\sqrt{\eta_1 \eta_2 S}} \right)^2.$$

これは (4.26) 式によって与えられた実現可能な最大値であることがわかる. 必然的に、この上限を得るために用いたすべての不等式で等号が成立しなければならない. それらの中で、(4.29) 式での三角不等式の等号はベクトル  $C$ ,  $X$  が同じ方向を向いていることを必要とする. そして、それは直ちに (4.27) 式の対称性を導く. (4.30) 式の等号は (4.28) 式の間接関係を要求する.

### 4.3 Single-state 領域

Unambiguous discrimination ( $m = 0$ ) の設定では、もし、生起確率が十分に小さければ、識別される状態の 1 つを除くことは最適であった. 一般のエラーマージンを持つ識別問題においても、パラメータ  $\eta_1$ ,  $m$  の領域で同じような状況が発生し、single-state 領域と呼ぶ. この節では、single-state 領域の最適な識別成功確率を決定する.

今、 $\eta_1 \leq \eta_2$  を仮定しているので、要素  $E_1 = 0$  を持つような最適な POVM を探す. すべての POVM 要素が多くてもランク 1 であることから、直ちに、要素  $E_2$ ,  $E_3$  は次のように決まった単位 Bloch ベクトル  $f$  を持つ正規直交状態の集合  $\{|f\rangle, | -f\rangle\}$  に関する射影測定を構成しなければならないことがわかる.

$$E_2 = |f\rangle\langle f|, \quad (4.31)$$

$$E_3 = | -f\rangle\langle -f|. \quad (4.32)$$

まず、(4.6) 式を見ると、(4.6a) 式は自明に満たされる. (4.6b), (4.6c) 式は次のようなことを要求する.

$$Y = \lambda_+ |f\rangle\langle f|, \quad (4.33)$$

$$Y - (\eta_2 \rho_2 - y \eta_1 \rho_1) = -\lambda_- | -f\rangle\langle -f|, \quad (4.34)$$

ここで、 $\lambda_+$ ,  $\lambda_-$  は定数である. また、(4.4a), (4.4c) 式から  $\lambda_+ \geq 0$ ,  $\lambda_- \leq 0$  であることがわかる. (4.33), (4.34) 式から  $Y$  を消去すると、次のような関係が得られる.

$$\eta_2 \rho_2 - y \eta_1 \rho_1 = \lambda_+ |f\rangle\langle f| + \lambda_- | -f\rangle\langle -f|.$$

これは演算子  $\eta_2 \rho_2 - y \eta_1 \rho_1$  のスペクトル分解である. そして、それは  $\lambda_+$ ,  $\lambda_-$  は固有状態  $|f\rangle$ ,  $| -f\rangle$  をそれぞれに持つ正と負の固有値であることを示す. したがって、 $\lambda_+$ ,  $\lambda_-$ ,  $f$  は Bloch ベクトル  $n_1$ ,  $n_2$  を用いて、次のように表すことができる.

$$\lambda_{\pm} = \frac{1}{2} (\eta_2 - y \eta_1) \pm \frac{1}{2} |a_2|, \quad (4.35)$$

$$f = \frac{a_2}{|a_2|}, \quad (4.36)$$

ここで、ベクトル  $\mathbf{a}_2$  は (4.13) 式で  $\mathbf{a}_2 = \eta_2 \mathbf{n}_2 - y\eta_1 \mathbf{n}_1$  として定義されている。

パラメータ  $y$  は (4.3c), (4.4b), (4.4d), (4.6d) 式を満たすように決定される。(4.4b) 式は演算子  $Y - (\eta_1 \rho_1 - y\eta_2 \rho_2)$  が正であることを示す。したがって、次のように表すことができる。

$$\lambda_+ - (\eta_1 - y\eta_2) \geq \left| \lambda_+ \frac{\mathbf{a}_2}{|\mathbf{a}_2|} - \mathbf{a}_1 \right|,$$

ここで、 $\mathbf{a}_1 = \eta_1 \mathbf{n}_1 - y\eta_2 \mathbf{n}_2$ ,  $\mathbf{a}_2 = \eta_2 \mathbf{n}_2 - y\eta_1 \mathbf{n}_1$  である。この不等式から、次のようなパラメータ  $y$  に関する 2 次不等式が得られる。

$$(\eta_1 - \eta_2 S) y^2 + 2\eta_2 T y + \frac{\eta_2}{\eta_1} (\eta_2 - \eta_1 S) \leq 0.$$

この 2 次不等式を解くことで、パラメータ  $y$  の許される範囲が決定される。ただし、 $y \geq 1$  であり、生起確率は次のような不等式を満たさなければならないことに注意しなければならない。

$$\eta_1 \leq \eta_2 S. \quad (4.37)$$

したがって、パラメータ  $y$  に対して、次のような不等式が成り立つ。

$$y \geq 1 + \frac{(1 - 2\sqrt{\eta_1 \eta_2 S}) \left(1 + \sqrt{\frac{\eta_2 S}{\eta_1}}\right)}{\eta_2 S - \eta_1}. \quad (4.38)$$

残りの条件式 (4.3c), (4.6d) はパラメータ  $y$  が (4.38) 式を満たさなければならないことから、 $p_{\times} = m$  という 1 つの方程式にすることができる。平均間違い確率  $p_{\times}$  は次のように計算できる。

$$p_{\times} = \eta_1 \text{tr}[E_2 \rho_1] = \eta_1 \frac{1 + \mathbf{f} \cdot \mathbf{n}_1}{2}.$$

これがエラーマージン  $m$  と等しくなければならない。そして、それは次のようなパラメータ  $y$  とエラーマージン  $m$  の間にある関係を明確に示す。

$$y = \frac{\eta_2}{\eta_1} \left( T - S + \sqrt{ST} \frac{\eta_1 - 2m}{\sqrt{m}(\eta_1 - m)} \right). \quad (4.39)$$

今、(4.38) 式で与えられたパラメータ  $y$  の許される範囲を次のようなエラーマージン  $m$  の許される範囲に書き換えることができる。

$$0 \leq m \leq \frac{(\eta_1 - \sqrt{\eta_1 \eta_2 S})^2}{1 - 2\sqrt{\eta_1 \eta_2 S}}. \quad (4.40)$$

(4.37), (4.40) 式を統合すると、single-state 領域が (4.10) 式で定義された  $m'_c$  を持つ不等式  $0 \leq m \leq m'_c$  によって定められることがわかる。

Single-state 領域の最大識別成功確率  $p_{\max}$  は  $d = \text{tr}[Y] + ym$  を計算することで次のように得られる。

$$p_{\max} = \eta_2 \left( \sqrt{\frac{m}{\eta_1}} S + \sqrt{\frac{\eta_1 - m}{\eta_1}} T \right)^2. \quad (4.41)$$

ここで、留意すべきことは  $m = 0$  ならば、これが  $\eta_1 \leq \eta_2 S$  での unambiguous discrimination に対するよく知られた結果  $p_o^{\max} = \eta_2 (1 - S) = \eta_2 (1 - |\langle \phi_1 | \phi_2 \rangle|^2)$  を再現していることである。

最後に、4.3 節では  $\eta_1 \leq \eta_2$  を仮定したが、 $\eta_1 \geq \eta_2$  の場合についても、 $E_2 = 0$  で状態  $\rho_2$  が除かれるような同様の single-state 領域があることは明らかである。

## 4.4 弱いエラーマージンと強いエラーマージン

ここまで、平均間違い確率  $p_{\times}$  に対してエラーマージン  $m$  を課して識別問題を考えてきた。一方、違う方法でエラーマージンを課して識別問題を考えることもできる。測定結果が  $\mu = 1$  であるとする、間違い確率は条件付き確率  $P_{\rho_2|E_1}$  で表すことができる。この節では、次のような 2 つの条件付き間違い確率がエラーマージン  $m$  を越えてはならないという条件を持つ識別問題を考察する。

$$P_{\rho_2|E_1} \leq m, \quad (4.42a)$$

$$P_{\rho_1|E_2} \leq m. \quad (4.42b)$$

これらの条件は (4.3c) 式が (4.42) 式から得られるという意味では前の節で考えたエラーマージンの条件よりも強いことがわかる。そして、それは次のように示すことができる。

$$\begin{aligned} p_{\times} &= P_{\rho_2, E_1} + P_{\rho_1, E_2} \\ &= P_{\rho_2|E_1} P_{E_1} + P_{\rho_1|E_2} P_{E_2} \\ &\leq m (P_{E_1} + P_{E_2}) \leq m. \end{aligned}$$

(4.3c), (4.42) 式によって与えられた条件をそれぞれ弱いエラーマージン条件、強いエラーマージン条件と呼ぶ。

生起確率が等しい場合、弱いエラーマージン条件と強いエラーマージン条件の両方について、最適な解はすでに得られている [17]。次に、一般の生起確率に関する 2 つのエラーマージン条件の最適な解の間にある関係について述べる。

強いエラーマージン条件と弱いエラーマージン条件の 2 つの設定を見分けるために、それぞれ上付き文字 S, W を用いて表す。まず、強いエラーマージン  $m^S$  を持つ最適な POVM  $E_{\mu}^S(m^S)$  から始める。平均間違い確率  $p_{\times}^S(m^S)$  を  $E_{\mu}^S(m^S)$  を用いて計算するとする。条件付き間違い確率を用いると、次のような関係が成立することに気づく。

$$\begin{aligned} p_{\times}^S(m^S) &= P_{\rho_2, E_1}^S(m^S) + P_{\rho_1, E_2}^S(m^S) \\ &= P_{\rho_2|E_1}^S(m^S) P_{E_1}^S(m^S) + P_{\rho_1|E_2}^S(m^S) P_{E_2}^S(m^S) \\ &\leq m^S (P_{E_1}^S(m^S) + P_{E_2}^S(m^S)) \\ &= m^S (p_{\max}^S(m^S) + p_{\times}^S(m^S)). \end{aligned}$$

したがって、それは次のような関係が成立することを示す。

$$p_{\times}^S(m^S) \leq \frac{m^S}{1 - m^S} p_{\max}^S(m^S).$$

これは強いエラーマージン  $m^S$  を持つ最適な POVM  $E_\mu^S(m^S)$  が  $m^W = \frac{m^S}{1-m^S} p_{\max}^S(m^S)$  を持つ弱いエラーマージン条件を満たすことを必要とする。したがって、2つの最大識別成功確率  $p_{\max}^S, p_{\max}^W$  に関する次のような不等式が得られる。

$$p_{\max}^S(m^S) \leq p_{\max}^W \left( \frac{m^S}{1-m^S} p_{\max}^S(m^S) \right). \quad (4.43)$$

$p_{\max}^S \leq p_{\max}^W$  はエラーマージン  $m$  の共通の値に対して成立することに注意しなければならない。なぜなら、強いエラーマージン条件は弱いエラーマージン条件よりも強いからである。しかしながら、ここで、(4.43) 式は異なる値のエラーマージンを含む。そして、それはこの不等式で実際に等号が成り立つことを示す。

さらに、2つの最大識別成功確率に関するもう1つの不等式を導くことができる。弱いエラーマージン  $m^W$  を満たすような最適な POVM  $E_\mu^W(m^W)$  をとるとする。Minimum-error 領域と intermediate 領域では、2つの条件付き間違い確率は  $P_{\rho_2|E_1}^W = P_{\rho_1|E_2}^W$  であった。一方、single-state 領域では、2つの条件付き確率のうちの1つは定義することができない。しかしながら、定数  $\kappa$  について次のような関係はまだ成立している。

$$\begin{aligned} P_{\rho_2, E_1}^W(m^W) &= \kappa P_{E_1}^W(m^W), \\ P_{\rho_1, E_2}^W(m^W) &= \kappa P_{E_2}^W(m^W). \end{aligned}$$

これら2つの関係式に加えて、次のような関係を得る。

$$p_{\times}^W(m^W) = \kappa [P_{E_1}^W(m^W) + P_{E_2}^W(m^W)] = \kappa [p_{\max}^W(m^W) + p_{\times}^W(m^W)].$$

したがって、それは次のような関係が成立することを示す。

$$\begin{aligned} \kappa &= \frac{p_{\times}^W(m^W)}{p_{\max}^W(m^W) + p_{\times}^W(m^W)} \\ &\leq \frac{m^W}{p_{\max}^W(m^W) + m^W}. \end{aligned}$$

これは弱いエラーマージンの設定での条件付き間違い確率が  $m^S = \frac{m^W}{p_{\max}^W(m^W) + m^W}$  を持つ強いエラーマージン条件を満たすことを示す。したがって、次のようなもう1つの不等式が得られる。

$$p_{\max}^W(m^W) \leq p_{\max}^S \left( \frac{m^W}{p_{\max}^W(m^W) + m^W} \right). \quad (4.44)$$

実際に、(4.43), (4.44) 式で等号は成り立つ。これは次のようにそれらを繰り返して使うことで見ることができる。

$$\begin{aligned} p_{\max}^S(m^S) &\leq p_{\max}^W \left[ \frac{m^S}{1-m^S} p_{\max}^S(m^S) \right] \\ &\leq p_{\max}^S \left\{ \frac{\frac{m^S}{1-m^S} p_{\max}^S(m^S)}{p_{\max}^W \left[ \frac{m^S}{1-m^S} p_{\max}^S(m^S) \right] + \frac{m^S}{1-m^S} p_{\max}^S(m^S)} \right\} \\ &\leq p_{\max}^S \left[ \frac{\frac{m^S}{1-m^S} p_{\max}^S(m^S)}{p_{\max}^S(m^S) + \frac{m^S}{1-m^S} p_{\max}^S(m^S)} \right] \\ &= p_{\max}^S(m^S). \end{aligned}$$



上の導出では, 成功確率はエラーマージンの増加関数であることを用いた.

したがって, もし, 2つのエラーマージン  $m^S, m^W$  が

$$m^S = \frac{m^W}{p_{\max}^W(m^W) + m^W}, \quad (4.45)$$

によって関係づけられるか,

$$m^W = \frac{m^S}{1 - m^S p_{\max}^S(m^S)}, \quad (4.46)$$

と同値であるならば, 2つの最大識別成功確率は等しい.

$$p_{\max}^S(m^S) = p_{\max}^W(m^W). \quad (4.47)$$

最大識別成功確率の1つを知っているとき, もう1つの最大識別成功確率はそれらの関係式によって決定することができる. また, 最適な POVM も同じ方法で  $E_{\mu}^S(m^S) = E_{\mu}^W(m^W)$  と関係づけられる.

上の関係を用いると, 強いエラーマージン条件での最大識別成功確率が次のように得られる.

$$p_{\max}^S = \begin{cases} \frac{1}{2} (1 + \sqrt{1 - 4\eta_1\eta_2 S}) & (m_c \leq m \leq 1), \\ A_m (1 - 2\sqrt{\eta_1\eta_2 S}) & (m'_c \leq m \leq m_c), \\ \frac{\eta_1\eta_2(1-m)(1-S)}{m\eta_1 + (1-m)\eta_1 - 2\sqrt{m(1-m)\eta_1\eta_2 S}} & (0 \leq m \leq m'_c), \end{cases} \quad (4.48)$$

ここで,  $A_m$  は次のように与えられる.

$$A_m = \frac{1-m}{(1-2m)^2} \left( 1 + 2\sqrt{m(1-m)} \right). \quad (4.49)$$

$\eta_1 \leq \eta_2$  を仮定し,  $m_c, m'_c$  は次のように定義される.

$$m_c \equiv \frac{1}{2} \left( 1 - \sqrt{1 - 4\eta_1\eta_2 S} \right), \quad (4.50)$$

$$m'_c \equiv \begin{cases} \frac{(\eta_1 - \sqrt{\eta_1\eta_2 S})^2}{(\eta_1 - \sqrt{\eta_1\eta_2 S})^2 + (\eta_2 - \sqrt{\eta_1\eta_2 S})^2} & (\eta_1 \leq \eta_2 S), \\ 0 & (\eta_1 \geq \eta_2 S). \end{cases} \quad (4.51)$$

## 4.5 混合状態に対する上限

識別される2つの状態  $\rho_1, \rho_2$  が混合状態の場合を考える. Minimum-error discrimination ( $m = 1$ ) の設定での最大識別成功確率は知られている. しかしながら, 一般の2つの混合状態の unambiguous discrimination ( $m = 0$ ) の設定では, 最大識別成功確率に対する解析的な結果は得られていない. Rudolph らは次のような簡単な識別成功確率に対する上限を与えた [42].

$$p_{\max}(\rho_1, \rho_2) \leq \begin{cases} 1 - 2\sqrt{\eta_1\eta_2} F(\rho_1, \rho_2) & (\eta_1 \geq \eta_2 F(\rho_1, \rho_2)^2), \\ \eta_2 (1 - F(\rho_1, \rho_2)^2) & (\eta_1 \leq \eta_2 F(\rho_1, \rho_2)^2), \end{cases} \quad (4.52)$$

ここで,  $F(\rho_1, \rho_2) = \text{tr}(\sqrt{\rho_1 \rho_2} \sqrt{\rho_1})^{1/2}$  は状態  $\rho_1$  と  $\rho_2$  の忠実度である. 最近, 上限に達するための 2 つの混合状態に対する条件が分析され, 新しい一連の上限も見つかった [43–46]. 一般のエラーマージンに対して, 最大識別成功確率の閉じた形式も unambiguous discrimination のように得るのは難しい. しかしながら, 上限は状態の忠実度と生起確率で表せられるので, (4.52) 式と似た上限が存在するのはもっともらしいことである. 次で, Rudolph らの方法が一般のエラーマージンの場合に適用できることを示し, 識別成功確率に対する上限が純粋状態の識別問題の結果を用いることで簡単に得ることができることを示す.

識別される状態は系  $Q$  に準備されているとし, もう 1 つの系  $R$  を導入することで次のように状態を純粋化する [41].

$$\rho_1^Q = \text{tr}_R |\Psi_1^{QR}\rangle \langle \Psi_1^{QR}|, \quad (4.53)$$

$$\rho_2^Q = \text{tr}_R |\Psi_2^{QR}\rangle \langle \Psi_2^{QR}|. \quad (4.54)$$

純粋状態  $|\Psi_1^{QR}\rangle, |\Psi_2^{QR}\rangle$  は次のような関係を満たすように選ばれたことを仮定する.

$$|\langle \Psi_1^{QR} | \Psi_2^{QR} \rangle| = F(\rho_1, \rho_2).$$

そして, それは Uhlmann の定理 [47] によって常に可能である.

生起確率  $\eta_1, \eta_2$  それぞれを持つ純粋状態  $|\Psi_1^{QR}\rangle, |\Psi_2^{QR}\rangle$  の仮定の識別問題を考える. そこで, 弱いエラーマージンの条件をとる. 課題は次のように与えられる識別成功確率

$$p_o = \eta_1 \text{tr}_{QR} E_1^{QR} |\Psi_1^{QR}\rangle \langle \Psi_1^{QR}| + \eta_2 \text{tr}_{QR} E_2^{QR} |\Psi_2^{QR}\rangle \langle \Psi_2^{QR}|, \quad (4.55)$$

を次のように与えられる平均の識別間違い確率

$$p_x = \eta_1 \text{tr}_{QR} E_2^{QR} |\Psi_1^{QR}\rangle \langle \Psi_1^{QR}| + \eta_2 \text{tr}_{QR} E_1^{QR} |\Psi_2^{QR}\rangle \langle \Psi_2^{QR}|, \quad (4.56)$$

がエラーマージン  $m$  を越えてはならないという条件の下で最大化することである. 2 つの純粋状態  $|\phi_1\rangle, |\phi_2\rangle$  に対する最大識別成功確率は  $|\langle \phi_1 | \phi_2 \rangle|$  の関数であり, 次元とは無関係である. そして, それを  $p_{\max}^{\text{pure}}(|\langle \phi_1 | \phi_2 \rangle|)$  によって表す. そのとき, 仮定の識別問題に対する最大識別成功確率は  $p_{\max}^{\text{pure}}[F(\rho_1, \rho_2)]$  によって与えられる.

この識別問題での  $E_\mu^{QR}$  に対して, 次のような追加の制限を課す.

$$E_\mu^{QR} = E_\mu^Q \otimes \mathbf{1}^R, \quad \mu = 1, 2, 3. \quad (4.57)$$

この追加の条件によって, 識別成功確率と平均の識別間違い確率は次のように変換される.

$$\begin{aligned} p_o &= \eta_1 \text{tr}_Q E_1^Q \rho_1^Q + \eta_2 \text{tr}_Q E_2^Q \rho_2^Q, \\ p_x &= \eta_1 \text{tr}_Q E_2^Q \rho_1^Q + \eta_2 \text{tr}_Q E_1^Q \rho_2^Q. \end{aligned}$$

そして, 問題は生起確率  $\eta_1, \eta_2$  それぞれを持つ 2 つの混合状態  $\rho_1, \rho_2$  の識別問題と等価となる. POVM に対するどんな追加条件も最大識別成功確率を増加させることは決してないことは明らかである. それゆえ, 2 つの混合状態に対する識別成功確率の上限が

2つの混合状態の忠実度により置き換えられた  $|\langle \phi_1 | \phi_2 \rangle|$  を持つ純粋状態の最大識別成功確率によって制約される。

$$p_{\max}(\rho_1, \rho_2) \leq p_{\max}^{\text{pure}}[F(\rho_1, \rho_2)].$$

したがって, (4.11) 式で与えられた純粋状態の場合の結果を用いると, 次のような結果が得られる。

$$p_{\max}(\rho_1, \rho_2) \leq \begin{cases} [\sqrt{m} + \sqrt{1 - 2\sqrt{\eta_1\eta_2}F(\rho_1, \rho_2)}]^2 & (m'_c \leq m \leq m_c), \\ \eta_2 \left\{ \sqrt{\frac{m}{\eta_1}} F(\rho_1, \rho_2) + \sqrt{\frac{\eta_1 - m}{\eta_1}} [1 - F(\rho_1, \rho_2)^2] \right\}^2 & (0 \leq m \leq m'_c), \end{cases}$$

ここで,  $m_c, m'_c$  は次のように与えられる。

$$m_c = \frac{1}{2} \left[ 1 - \sqrt{1 - 4\eta_1\eta_2 F(\rho_1, \rho_2)^2} \right],$$

$$m'_c = \begin{cases} \frac{[\eta_1 - \sqrt{\eta_1\eta_2}F(\rho_1, \rho_2)]^2}{1 - 2\sqrt{\eta_1\eta_2}F(\rho_1, \rho_2)} & [\eta_1 \leq \eta_2 F(\rho_1, \rho_2)^2], \\ 0 & [\eta_1 \geq \eta_2 F(\rho_1, \rho_2)^2], \end{cases}$$

ただし, 純粋状態の場合のように,  $\eta_1 \leq \eta_2$  を仮定したことに注意しなければならない。

Unambiguous discrimination ( $m = 0$ ) に対して, 上限は (4.52) 式で与えられたそれに帰着する。一方, minimum-error discrimination の最大識別成功確率は知られており, 次のように与えられる。

$$p_{\max}(\rho_1, \rho_2) = \frac{1}{2} (1 + \text{tr} |\eta_1 \rho_1 - \eta_2 \rho_2|).$$

そして, それは上限を越えてはならないので, 次のような不等式を導く。

$$\text{tr} |\eta_1 \rho_1 - \eta_2 \rho_2| \leq \sqrt{1 - 4\eta_1\eta_2 F(\rho_1, \rho_2)^2}.$$

さらに, それは次のようなトレース距離と忠実度についての不等式の一般化である [41].

$$\frac{1}{2} \text{tr} |\rho_1 - \rho_2| \leq \sqrt{1 - F(\rho_1, \rho_2)^2}.$$

## 第5章 3つの純粋状態の minimum-error discrimination

識別が間違ふ確率に対して何の制限もなしに識別成功確率を最大にする minimum-error discrimination を考える. 直接, 与えられた主問題を解くのではなく, そこから導かれた双対問題を解くことで最大識別成功確率とそれを達成する最適な測定を解析的に求める. 生起確率が等しい qubit の 3 つの純粋状態の場合を分析し, 識別される状態の Bloch ベクトルそれぞれの終点がなす三角形の外心が最適な解の構成に重要な役割を果たすことがわかった. さらに, 一般の生起確率を持つ qubit の 3 つの純粋状態の場合に拡張する.

### 5.1 問題の定式化

それぞれ生起確率  $\eta_i$  を持つ純粋状態  $\rho_i$  ( $i = 1, 2, \dots, n$ ) の minimum-error discrimination を考える. 生起確率  $\eta_i$  はゼロではなく,  $\sum_{i=1}^n \eta_i = 1$  であることを仮定する. Minimum-error discrimination の設定での課題は識別が間違ふ確率に対して, 何の制限もなしに識別成功確率を最大にすることである.

測定は POVM によって記述され,  $n$  個の要素  $\{E_1, E_2, \dots, E_n\}$  から成り立つ.  $i = 1, 2, \dots, n$  で得られる測定結果は与えられた状態が  $\rho_i$  であると同定することを表す.

識別成功確率  $p_\circ$  は次のように与えられる.

$$p_\circ = \sum_{i=1}^n \eta_i \text{tr}[E_i \rho_i], \quad (5.1)$$

課題は次のような条件の下で識別成功確率  $p_\circ$  を最大にすることである.

$$E_i \geq 0 \quad (i = 1, 2, \dots, n), \quad (5.2a)$$

$$\sum_{i=1}^n E_i = I, \quad (5.2b)$$

ここで, (5.2a), (5.2b) 式は  $E_i$  が POVM であるための条件である. このように Minimum-error discrimination は semidefinite programming (SDP) の 1 つとして定式化される [37–39].

一方, 次のような条件を満たす Hermite 演算子  $Y$  が存在するとする.

$$Y \geq \eta_i \rho_i (i = 1, 2, \dots, n). \quad (5.3)$$

このとき, 次のように定義された

$$d \equiv \text{tr}[Y], \quad (5.4)$$

が識別成功確率  $p_o$  に対して上限を与えることは次のように示される.

$$\begin{aligned} p_o &= \sum_{i=1}^n \text{tr}[E_i \eta_i \rho_i] \\ &\leq \sum_{i=1}^n \text{tr}[E_i Y] = \text{tr}[Y] = d. \end{aligned}$$

次のような実現可能条件を満たす場合に限り, この不等式の等号が成り立つ.

$$E_i(Y - \eta_i \rho_i) = 0 \quad (i = 1, 2, \dots, n). \quad (5.5)$$

条件式 (5.3) の下で  $d$  を最小にすることを双対問題と呼び, 最初の問題である条件式 (5.2a), (5.2b) の下で  $p_o$  を最大にすることを主問題と呼ぶ.

最適な解を得るための戦略では, 直接, 主問題を解くのではなく, そこから導かれた双対問題を解くことで最大識別成功確率を求める. そのとき, (5.2a), (5.2b), (5.5) 式を満たすように POVM $\{E_i\}$  を構成する.

## 5.2 2つの純粋状態の場合

3.2 節でも見たように, 2つの純粋状態の minimum-error discrimination の最適な解はよく知られている [2]. 3.2 節では, 主問題を解くことで最大識別成功確率が得られた. 今節では, 別の方法として, 双対問題を解くことで最大識別成功確率を解析的に求める. そして, それを達成し, (5.2a), (5.2b), (5.5) 式を満たすような最適な POVM を構成する.

双対問題の課題は

$$d = \text{tr}[Y], \quad (5.6)$$

を次のような条件下で最小にすることである.

$$Y \geq \eta_1 \rho_1, \quad (5.7a)$$

$$Y \geq \eta_2 \rho_2, \quad (5.7b)$$

ここで,  $Y$  は  $2 \times 2$  Hermite 行列である. (5.7a), (5.7b) 式によって与えられた条件は次のように定義される演算子

$$Y_1 \equiv Y - \eta_1 \rho_1,$$

$$Y_2 \equiv Y - \eta_2 \rho_2,$$

が半正定値性を持つことを意味する。状態  $\rho_i$  やその他の演算子に対して Bloch ベクトル表示を用いると便利である。

$$\rho_i = \frac{1 + \mathbf{n}_i \cdot \boldsymbol{\sigma}}{2} \quad (i = 1, 2),$$

ここで,  $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$  は Pauli 行列である。さらに, 演算子  $Y$  は次のように表すことができる。

$$Y = \frac{\alpha + \boldsymbol{\beta} \cdot \boldsymbol{\sigma}}{2}$$

したがって, 演算子  $Y_1, Y_2$  は次のように書き換えられる。

$$\begin{aligned} Y_1 &= \frac{1}{2} [\alpha - \eta_1 + (\boldsymbol{\beta} - \eta_1 \mathbf{n}_1) \cdot \boldsymbol{\sigma}], \\ Y_2 &= \frac{1}{2} [\alpha - \eta_2 + (\boldsymbol{\beta} - \eta_2 \mathbf{n}_2) \cdot \boldsymbol{\sigma}]. \end{aligned}$$

演算子  $Y_1, Y_2$  は半正定値性を持つことから, それぞれの小さい方の固有値は正でなければならない。それゆえ, 次のような  $\alpha$  と  $\boldsymbol{\beta}$  に対する 2 つの不等式が得られる。

$$\begin{aligned} \alpha &\geq \eta_1 + |\boldsymbol{\beta} - \eta_1 \mathbf{n}_1|, \\ \alpha &\geq \eta_2 + |\boldsymbol{\beta} - \eta_2 \mathbf{n}_2|. \end{aligned}$$

さらに,  $d$  も次のように書き換えられる。

$$d = \text{tr} \left[ \frac{\alpha + \boldsymbol{\beta} \cdot \boldsymbol{\sigma}}{2} \right] = \alpha.$$

したがって, 双対問題はパラメータ  $\{\alpha, \boldsymbol{\beta}\}$  で次のように書き換えられる。

minimize :

$$d = \alpha, \tag{5.8a}$$

subject to :

$$\alpha \geq \eta_1 + |\boldsymbol{\beta} - \eta_1 \mathbf{n}_1|, \tag{5.8b}$$

$$\alpha \geq \eta_2 + |\boldsymbol{\beta} - \eta_2 \mathbf{n}_2|. \tag{5.8c}$$

(5.8b), (5.8c) 式で与えられた条件から,  $d$  は次のように与えられる。

$$d = \alpha = \max \{ \eta_1 + |\boldsymbol{\beta} - \eta_1 \mathbf{n}_1|, \eta_2 + |\boldsymbol{\beta} - \eta_2 \mathbf{n}_2| \}, \tag{5.9}$$

ここで,  $\max \{ \cdot, \cdot \}$  は 2 値のうちの大きい方の値をとることを表す表記である。一般に, 2 値のうちの大きい方の値は 2 値の平均値よりも大きいことから, 次のような不等式が成り立つ。

$$\max \{ \eta_1 + |\boldsymbol{\beta} - \eta_1 \mathbf{n}_1|, \eta_2 + |\boldsymbol{\beta} - \eta_2 \mathbf{n}_2| \} \geq \frac{\eta_1 + |\boldsymbol{\beta} - \eta_1 \mathbf{n}_1| + \eta_2 + |\boldsymbol{\beta} - \eta_2 \mathbf{n}_2|}{2}$$

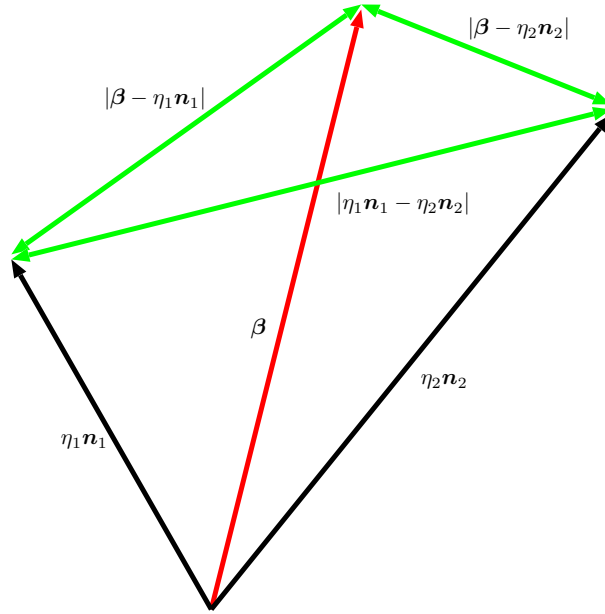


図 5.1: 3 つのベクトルの距離

また, 図 5.1 のように 3 つのベクトル  $\beta$ ,  $\eta_1 \mathbf{n}_1$ ,  $\eta_2 \mathbf{n}_2$  の終点は三角形をなす. それゆえ, 三角不等式を用いると, 3 つのベクトル間の距離には次のような関係が成り立つ.

$$|\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2| \leq |\beta - \eta_1 \mathbf{n}_1| + |\beta - \eta_2 \mathbf{n}_2|.$$

したがって, 次のような関係が成り立つことがわかる.

$$\begin{aligned} \max \{ \eta_1 + |\beta - \eta_1 \mathbf{n}_1|, \eta_2 + |\beta - \eta_2 \mathbf{n}_2| \} &\geq \frac{1 + |\beta - \eta_1 \mathbf{n}_1| + |\beta - \eta_2 \mathbf{n}_2|}{2} \\ &\geq \frac{1 + |\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2|}{2}. \end{aligned}$$

この最後の行の不等式は  $d$  の下限を与える. それはこの不等式で等号が成り立つようにベクトル  $\beta$  を決定すればよいことを意味する. それゆえ, この下限を達成するために, 次のような条件を満たすベクトル  $\beta$  を見つける.

$$\eta_1 + |\beta - \eta_1 \mathbf{n}_1| = \eta_2 + |\beta - \eta_2 \mathbf{n}_2|, \quad (5.10)$$

$$|\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2| = |\beta - \eta_1 \mathbf{n}_1| + |\beta - \eta_2 \mathbf{n}_2|. \quad (5.11)$$

(5.10), (5.11) 式の和と差から, 次のような関係が得られる.

$$|\beta - \eta_1 \mathbf{n}_1| = \frac{\eta_2 - \eta_1 + |\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2|}{2}, \quad (5.12)$$

$$|\beta - \eta_2 \mathbf{n}_2| = \frac{\eta_1 - \eta_2 + |\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2|}{2}. \quad (5.13)$$

(5.11) 式はベクトル  $\beta$  の終点が図 5.2 のようにベクトル  $\eta_1 \mathbf{n}_1$  の終点とベクトル  $\eta_2 \mathbf{n}_2$  の終点を結ぶ直線上にあることを意味する. それゆえ, ベクトル  $\beta$  は次のように表すことができる.

$$\beta = \eta_1 \mathbf{n}_1 + |\beta - \eta_2 \mathbf{n}_2| \mathbf{m} = \eta_2 \mathbf{n}_2 - |\beta - \eta_1 \mathbf{n}_1| \mathbf{m}, \quad (5.14)$$

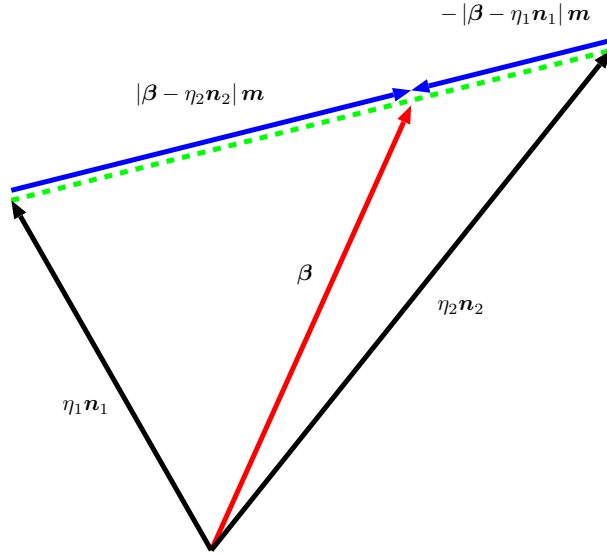


図 5.2: 最適なベクトル  $\beta$

ここで、次のように定義されたベクトル  $m$  を導入した.

$$m \equiv \frac{\eta_1 n_1 - \eta_2 n_2}{|\eta_1 n_1 - \eta_2 n_2|}. \quad (5.15)$$

さらに、(5.12), (5.13) 式を用いると、ベクトル  $\beta$  は次のように書き換えられる.

$$\beta = \frac{\eta_1}{2} \left( 1 + \frac{\eta_1 - \eta_2}{|\eta_1 n_1 - \eta_2 n_2|} \right) n_1 + \frac{\eta_2}{2} \left( 1 - \frac{\eta_1 - \eta_2}{|\eta_1 n_1 - \eta_2 n_2|} \right) n_2. \quad (5.16)$$

そして、 $d_{\min}$  は次のように与えられる.

$$d_{\min} = \alpha = \frac{1}{2} (1 + |\eta_1 n_1 - \eta_2 n_2|). \quad (5.17)$$

もし、 $\eta_1 = \eta_2 = 1/2$  であるならば、(5.16) 式で与えられたベクトル  $\beta$  の終点はベクトル  $\eta_1 n_1$ ,  $\eta_2 n_2$  それぞれの終点を結ぶ直線の中点にあることは明らかである. この事実は次節の 3 つの純粋状態の場合の解法に対して、重要なヒントを与える.

(5.5) 式で与えられた実現可能条件は POVM 要素  $E_1$ ,  $E_2$  が次のような形式で与えられることを意味する.

$$E_1 = C_1 |m\rangle\langle m|, \quad E_2 = C_2 |-m\rangle\langle -m|,$$

ここで、ベクトル  $m$  は (5.15) 式で定義された単位ベクトルである. (5.2a), (5.2b) 式を満たすように係数  $C_1$ ,  $C_2$  を決定する. まず、(5.2b) 式で与えられる POVM の完全性関係から、係数  $C_1$ ,  $C_2$  に対して次のような関係が成り立つ.

$$\frac{1}{2} (C_1 + C_2) = 1, \quad (5.18)$$

$$C_1 m - C_2 m = 0. \quad (5.19)$$



この2つの関係式から,  $C_1 = C_2 = 1$  であることは明らかである. さらに,  $C_1, C_2 > 0$  であることから, (5.2a) 式も満たされる.

したがって, (5.17) 式を達成する最適な POVM 要素  $E_1, E_2$  は次のように与えられる.

$$E_1 = \frac{1}{2} \left( 1 + \frac{\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2}{|\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2|} \right), \quad E_2 = \frac{1}{2} \left( 1 - \frac{\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2}{|\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2|} \right). \quad (5.20)$$

以上から, (5.17) 式で与えられた上限を達成する POVM が構成され, 最大識別成功確率  $p_{\max}$  は次のように与えられる.

$$p_{\max} = \frac{1}{2} (1 + |\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2|). \quad (5.21)$$

この最大識別成功確率は 3.1 節でも得られた 2 つの純粋状態の minimum-error discrimination のよく知られた結果を再現している.

### 5.3 生起確率が等しい qubit の 3 つの純粋状態の場合

今節では, 生起確率  $\eta_1 = \eta_2 = \eta_3 = 1/3$  を持つ qubit の 3 つの純粋状態  $\rho_i = |\phi_i\rangle\langle\phi_i|$  の場合を考える. このとき, 双対問題の課題は

$$d = \text{tr}[Y], \quad (5.22a)$$

を次のような条件の下で最小化することである.

$$Y \geq \frac{1}{3} \rho_1, \quad (5.22b)$$

$$Y \geq \frac{1}{3} \rho_2, \quad (5.22c)$$

$$Y \geq \frac{1}{3} \rho_3. \quad (5.22d)$$

今, 識別される状態は qubit であることから, 状態  $\rho_i$  やその他の演算子に対して Bloch ベクトル表示を用いると便利である.

$$\rho_i = \frac{1 + \mathbf{n}_i \cdot \boldsymbol{\sigma}}{2} \quad (i = 1, 2, 3).$$

さらに,  $Y$  は  $2 \times 2$  Hermite 演算子であることから, 次のように与えられる.

$$Y = \frac{\alpha + \boldsymbol{\beta} \cdot \boldsymbol{\sigma}}{2}.$$

また, (5.22b), (5.22c), (5.22d) 式で与えられた条件は次のように定義される

$$\begin{aligned} Y_1 &\equiv \frac{1}{2} \left[ \alpha - \frac{1}{3} + \left( \boldsymbol{\beta} - \frac{1}{3} \mathbf{n}_1 \right) \cdot \boldsymbol{\sigma} \right], \\ Y_2 &\equiv \frac{1}{2} \left[ \alpha - \frac{1}{3} + \left( \boldsymbol{\beta} - \frac{1}{3} \mathbf{n}_2 \right) \cdot \boldsymbol{\sigma} \right], \\ Y_3 &\equiv \frac{1}{2} \left[ \alpha - \frac{1}{3} + \left( \boldsymbol{\beta} - \frac{1}{3} \mathbf{n}_3 \right) \cdot \boldsymbol{\sigma} \right], \end{aligned}$$

が半正定値性を持つことを意味する。それゆえ、 $Y_1, Y_2, Y_3$  それぞれの小さい方の固有値は正でなければならない。

したがって、双対問題は Bloch ベクトル表示を用いて、次のように書き換えられる。

minimize :

$$d = \alpha, \quad (5.23a)$$

subject to :

$$\alpha \geq \frac{1}{3} + \left| \beta - \frac{1}{3} \mathbf{n}_1 \right|, \quad (5.23b)$$

$$\alpha \geq \frac{1}{3} + \left| \beta - \frac{1}{3} \mathbf{n}_2 \right|, \quad (5.23c)$$

$$\alpha \geq \frac{1}{3} + \left| \beta - \frac{1}{3} \mathbf{n}_3 \right|. \quad (5.23d)$$

生起確率が等しい 2 つの純粋状態の場合、最適なベクトル  $\beta$  の終点は 2 つのベクトル  $\mathbf{n}_1/2, \mathbf{n}_2/2$  それぞれの終点を結ぶ直線の中点であった。この事実是最適なベクトル  $\beta$  の終点が生起確率が等しい qubit の 3 つの純粋状態の場合では、三角形をなす 3 つのベクトル  $\mathbf{n}_1/3, \mathbf{n}_2/3, \mathbf{n}_3/3$  それぞれの終点から等距離にある三角形の外心であることを予期させる。それゆえ、今後、最適なベクトル  $\beta$  の終点は三角形の終点であることを仮定して議論する。

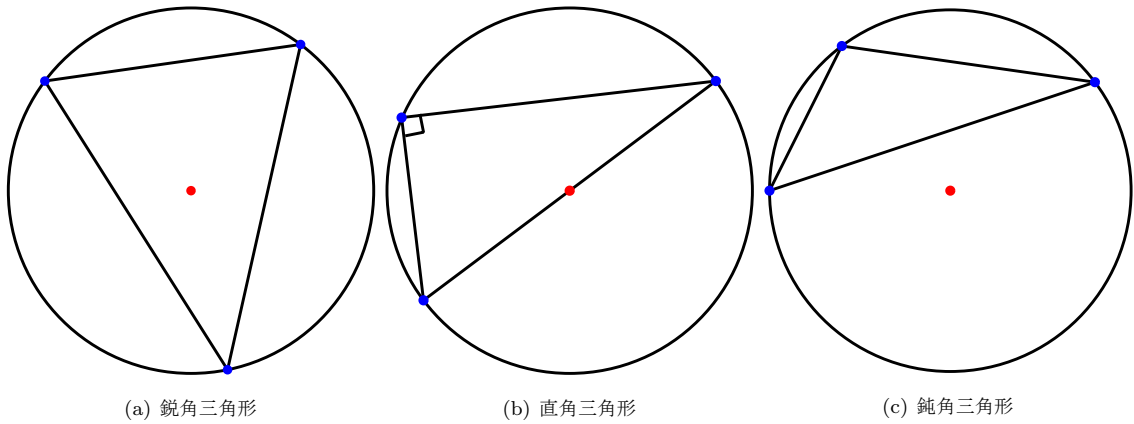


図 5.3: 三角形と外心の位置

図 5.3 のように、三角形の形状によって外心の位置は変化する。そこで、2 つの場合が考えられる。1 つは外心が外周上を含む三角形の内部に存在する場合である。もう 1 つは外心が三角形の外部に存在する場合である。次の小節では、外心が外周上を含む三角形の内部に存在する場合、外心が三角形の外部に存在する場合それぞれについて、詳しく分析し、最大識別成功確率とそれを達成する POVM を構成する。

### 5.3.1 外心が外周上を含む三角形の内部に存在する場合

外心が外周上を含む三角形の内部に存在するための条件として、3つのベクトル  $\mathbf{n}_1/3$ ,  $\mathbf{n}_2/3$ ,  $\mathbf{n}_3/3$  それぞれの終点がなす三角形が鋭角三角形または直角三角形でなければならない。つまり、次のような条件を満たす場合である。

$$(\mathbf{n}_3 - \mathbf{n}_1) \cdot (\mathbf{n}_2 - \mathbf{n}_1) \geq 0, \quad (5.24a)$$

$$(\mathbf{n}_1 - \mathbf{n}_2) \cdot (\mathbf{n}_3 - \mathbf{n}_2) \geq 0, \quad (5.24b)$$

$$(\mathbf{n}_2 - \mathbf{n}_3) \cdot (\mathbf{n}_1 - \mathbf{n}_3) \geq 0. \quad (5.24c)$$

まず、最適なベクトル  $\beta$  の終点が外心に存在することを示す。図 5.4 のように、三角形の各頂点を中心とし、外心と各頂点との距離を半径とする 3 つの円があったとする。ただし、この 3 つの円は外心でのみ交わる。今、外心と三角形の各頂点との距離よりも各頂点との距離がすべて小さくなるような点が存在すれば、その点がより小さい上限  $d$  を与えることは明らかである。しかしながら、図 5.4 を見れば、そのような点は存在しないことが直観的にわかる。それゆえ、最適なベクトル  $\beta$  の終点は外心に存在することがわかる。

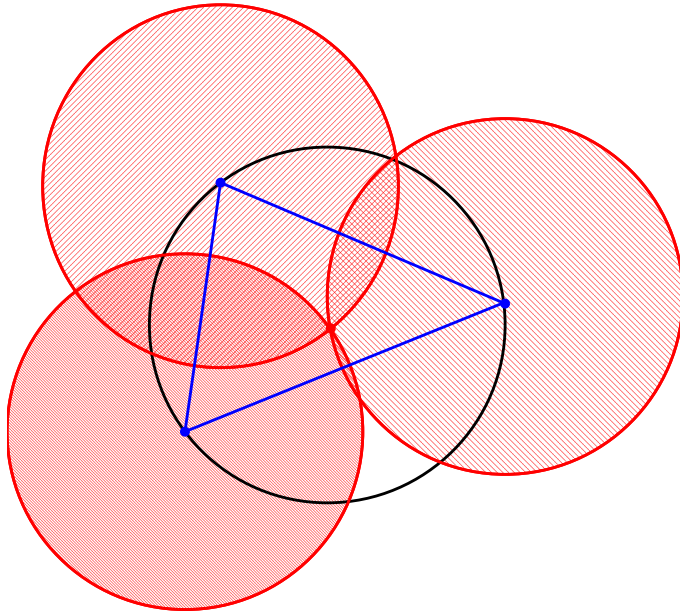


図 5.4: 外心と三角形の各頂点との距離を半径とする 3 つの円

それは次のようにしてより厳密に証明される。外心と三角形の各頂点との距離よりも各頂点との距離がすべて小さくなるような外心から  $\Delta\beta (\neq 0)$  だけずらした点が存在するとする。そのとき、図 5.5 のように、外心を終点とするベクトルを  $\beta$  とすると、外心から  $\Delta\beta (\neq 0)$  だけずらした点を終点とするベクトル  $\beta'$  は次のように与えられる。

$$\beta' = \beta + \Delta\beta.$$

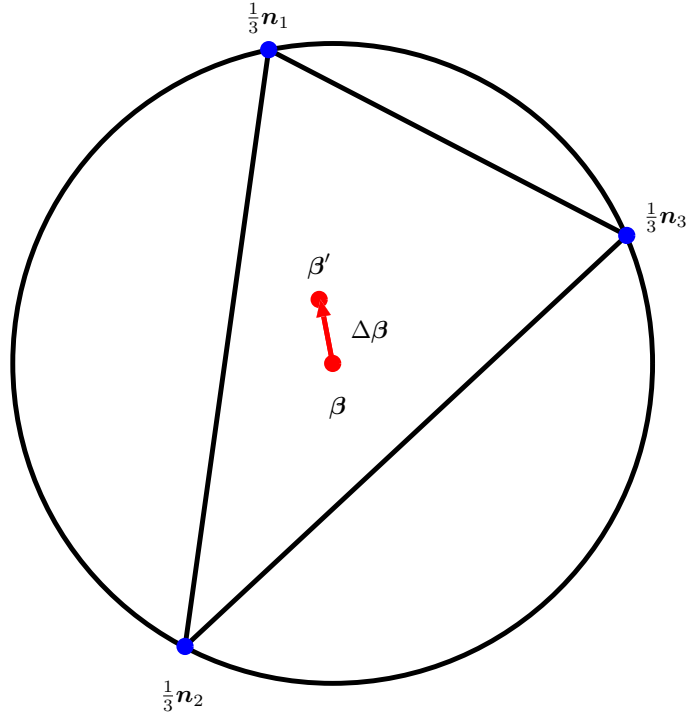


図 5.5: ベクトル  $\beta$  の終点から  $\Delta\beta$  だけずらしたベクトル  $\beta'$  の終点 (1)

仮定から, ベクトル  $\beta$  と三角形の各頂点との距離とベクトル  $\beta'$  と三角形の各頂点との距離には次のような関係が成り立つ.

$$\begin{aligned} \left| \beta - \frac{1}{3}n_1 \right| &> \left| \beta' - \frac{1}{3}n_1 \right|, \\ \left| \beta - \frac{1}{3}n_2 \right| &> \left| \beta' - \frac{1}{3}n_2 \right|, \\ \left| \beta - \frac{1}{3}n_3 \right| &> \left| \beta' - \frac{1}{3}n_3 \right|. \end{aligned}$$

さらに, この不等式は次のように書き換えられることは明らかである.

$$\begin{aligned} \left| \beta - \frac{1}{3}n_1 \right| &> \left| \beta - \frac{1}{3}n_1 + \Delta\beta \right|, \\ \left| \beta - \frac{1}{3}n_2 \right| &> \left| \beta - \frac{1}{3}n_2 + \Delta\beta \right|, \\ \left| \beta - \frac{1}{3}n_3 \right| &> \left| \beta - \frac{1}{3}n_3 + \Delta\beta \right|. \end{aligned}$$

今, 任意のベクトル  $a, b$  に対して Schwarz の不等式を適用すると, 次のような関係が成り立つ.

$$|a + b| \geq |b| + \frac{a \cdot b}{|b|}. \quad (5.25)$$

(5.25) 式を先ほどの不等式に対して適用すると、次のような不等式が与えられる。

$$\begin{aligned} 0 &> \left(\beta - \frac{1}{3}n_1\right) \cdot \Delta\beta, \\ 0 &> \left(\beta - \frac{1}{3}n_2\right) \cdot \Delta\beta, \\ 0 &> \left(\beta - \frac{1}{3}n_3\right) \cdot \Delta\beta. \end{aligned}$$

この不等式に対して、それぞれ任意の実数  $x, y, z$  を掛けて和をとると、次のような不等式が得られる。

$$0 > \left[(x + y + z)\beta - \left(x\frac{n_1}{3} + y\frac{n_2}{3} + z\frac{n_3}{3}\right)\right] \cdot \Delta\beta. \quad (5.26)$$

一般に、ベクトル  $\beta$  の終点が外周上を含む三角形の内部にある場合、ベクトル  $\beta$  は次のような形式で与えられる。

$$\beta = x\frac{n_1}{3} + y\frac{n_2}{3} + z\frac{n_3}{3},$$

ここで、 $x, y, z$  は  $x \geq 0, y \geq 0, z \geq 0$  であり、 $x + y + z = 1$  を満たす実数である。それゆえ、(5.26) 式で与えられる不等式は次のように書き換えられる。

$$0 > 0 \cdot \Delta\beta. \quad (5.27)$$

この不等式は明らかに矛盾している。それゆえ、最初の仮定である外心と三角形の各頂点との距離よりも各頂点との距離がすべて小さくなるような外心から  $\Delta\beta (\neq 0)$  だけずらした点が存在するということが矛盾していることになる。したがって、最適なベクトル  $\beta$  の終点は外心に存在することが示された。

今、最適なベクトル  $\beta$  の終点は外心であることから、付録 B を参照すると、ベクトル  $\beta$  は次のように与えられることがわかる。

$$\beta = -\frac{1}{24S^2} \left[ (|a|^2 b \cdot c) n_1 + (|b|^2 c \cdot a) n_2 + (|c|^2 a \cdot b) n_3 \right], \quad (5.28)$$

ここで、3 つのベクトル  $a, b, c$  は Bloch ベクトル  $n_1, n_2, n_3$  を用いて次のように定義される。

$$a \equiv \frac{1}{3}(n_3 - n_2), \quad b \equiv \frac{1}{3}(n_1 - n_3), \quad c \equiv \frac{1}{3}(n_2 - n_1). \quad (5.29)$$

また、(5.24) 式で与えられた 3 つのベクトル  $n_1/3, n_2/3, n_3/3$  それぞれの終点がなす三角形が鋭角三角形または直角三角形である条件から、次のような関係が得られる。

$$a \cdot b < 0, \quad b \cdot c < 0, \quad c \cdot a < 0. \quad (5.30)$$

それゆえ、(5.28) 式で与えられた最適なベクトル  $\beta$  の Bloch ベクトル  $n_1, n_2, n_3$  の係数は全体で正であることに注意しなければならない。

さらに、三角形の各頂点との距離は外接円の半径  $R$  を用いて、次のように表すことができる。

$$\left| \beta - \frac{1}{3} \mathbf{n}_1 \right| = \left| \beta - \frac{1}{3} \mathbf{n}_2 \right| = \left| \beta - \frac{1}{3} \mathbf{n}_3 \right| = R, \quad (5.31)$$

ここで、付録 B を参照すると、外接円の半径  $R$  は次のように与えられる。

$$R = \frac{|\mathbf{a}| |\mathbf{b}| |\mathbf{c}|}{4S}. \quad (5.32)$$

したがって、上限  $d$  の最小値は次のように与えられる。

$$d_{\min} = \alpha = \frac{1}{3} + R. \quad (5.33)$$

(5.33) 式で与えられる上限  $d$  を達成する POVM を構成する。(5.5) 式で与えられた実現可能条件は POVM 要素  $E_i$  が次のような形式で与えられることを意味する。

$$E_i = C_i \frac{1 - \mathbf{m}_i \cdot \boldsymbol{\sigma}}{2} \quad (i = 1, 2, 3),$$

ここで、ベクトル  $\mathbf{m}_i$  は次のように定義された単位ベクトルである。

$$\mathbf{m}_i \equiv \frac{1}{R} \left( \beta - \frac{1}{3} \mathbf{n}_i \right) \quad (i = 1, 2, 3).$$

ただし、ベクトル  $\beta$  は (5.28) 式で与えられる。

問題は (5.2a), (5.2b) 式を満たすように係数  $C_i$  を決定することである。(5.2b) 式で与えられる POVM の完全性関係から、係数  $C_i$  に対して次のような関係が成り立つ。

$$\frac{1}{2} (C_1 + C_2 + C_3) = 1, \quad (5.34)$$

$$C_1 \mathbf{m}_1 + C_2 \mathbf{m}_2 + C_3 \mathbf{m}_3 = 0. \quad (5.35)$$

(5.35) 式で、3 つのベクトル  $\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3$  は Bloch ベクトル  $\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3$  を用いて表すことができる。それゆえ、(5.34), (5.35) 式から次のような関係が得られる。

$$\beta = \frac{1}{6} (C_1 \mathbf{n}_1 + C_2 \mathbf{n}_2 + C_3 \mathbf{n}_3). \quad (5.36)$$

今、ベクトル  $\beta$  は (5.28) 式で与えられる。したがって、係数比較することで、係数  $C_i$  はそれぞれ次のように与えられる。

$$C_1 = -\frac{1}{4S^2} (|\mathbf{a}|^2 \mathbf{b} \cdot \mathbf{c}), \quad C_2 = -\frac{1}{4S^2} (|\mathbf{b}|^2 \mathbf{c} \cdot \mathbf{a}), \quad C_3 = -\frac{1}{4S^2} (|\mathbf{c}|^2 \mathbf{a} \cdot \mathbf{b}),$$

ここで、(5.30) 式で与えられた関係から、係数  $C_1, C_2, C_3$  は全体として正であることがわかる。それゆえ、(5.2a) 式を満たすことは明らかである。

以上から、(5.33) 式で与えられる上限を達成する POVM が構成できた。そして、最大識別成功確率は次のように与えられる。

$$p_{\max} = \frac{1}{3} + R. \quad (5.37)$$

ただし、 $R$  は 3 つのベクトル  $\mathbf{n}_1/3, \mathbf{n}_2/3, \mathbf{n}_3/3$  それぞれの終点がなす三角形の外接円の半径である。

### 5.3.2 外心が三角形の外部に存在する場合

外心が三角形の外部に存在する場合, 3つのベクトル  $n_1/3$ ,  $n_2/3$ ,  $n_3/3$  それぞれの終点がなす三角形は鈍角三角形である. すなわち, それは次のような3つの条件のうち, どれか1つを満たす場合である.

$$(n_3 - n_1) \cdot (n_2 - n_1) < 0, \quad (5.38a)$$

$$(n_1 - n_2) \cdot (n_3 - n_2) < 0, \quad (5.38b)$$

$$(n_2 - n_3) \cdot (n_1 - n_3) < 0. \quad (5.38c)$$

今, (5.38a) 式が満たされる場合を考えると, 外心が外周上を含む三角形の内部に存在する場合, ベクトル  $\beta$  の終点が外心にある場合が最適であった. しかしながら, 外心が三角形の外部に存在する場合, 必ずしも, ベクトル  $\beta$  の終点が外心にある場合が最適であるとは言えない. それは次のようにして示すことができる.

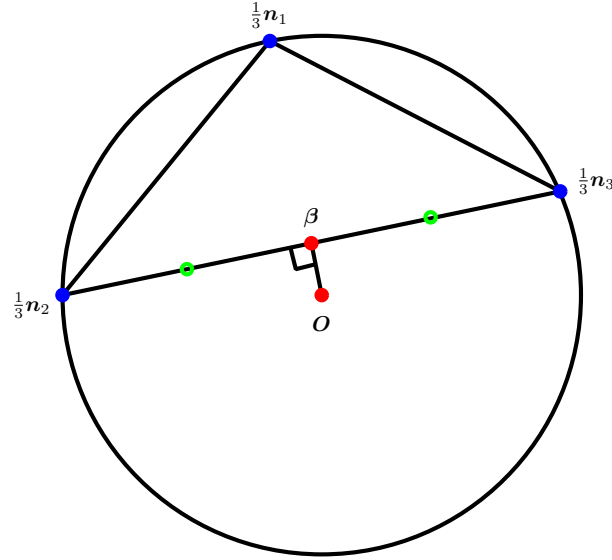


図 5.6: 外心から一番近い三角形の辺への垂線との交点

図 5.6 のように, 外心から一番近い三角形の辺に対して垂線を下ろし, その交点を終点としたベクトルを  $\beta$  とする. また, その交点はその辺を2等分する中点である. これは外心が各辺の垂直二等分線の交点であることから明らかである. それゆえ, ベクトル  $\beta$  は次のように与えられる.

$$\beta = \frac{1}{6} (n_2 + n_3). \quad (5.39)$$

図 5.6 からわかるように, このベクトル  $\beta$  の終点と三角形の各頂点との距離は外心と三角形の各頂点との距離よりも明らかに小さい. それゆえ, (5.39) 式で与えられたベクトル  $\beta$  の方がより小さい上限  $d$  を与えることがわかる. また, ベクトル  $\beta$  と三角形の各頂点との距離には次のような関係が成り立つことに注意しなければならない.

$$\left| \beta - \frac{1}{3} n_2 \right| = \left| \beta - \frac{1}{3} n_3 \right| > \left| \beta - \frac{1}{3} n_1 \right|. \quad (5.40)$$

次に, (5.39) 式で与えられたベクトル  $\beta$  が最適であることを示す. ベクトル  $\beta$  の終点と三角形の各頂点との距離よりも各頂点との距離がすべて小さくなるような点が存在するとする. そして, その点を終点とするベクトルを  $\beta'$  とすると, ベクトル  $\beta'$  は図 5.7 のようにベクトル  $\beta$  の終点から  $\Delta\beta (\neq 0)$  だけずらした点が終点であるベクトルで与えられるとする.

$$\beta' = \beta + \Delta\beta.$$

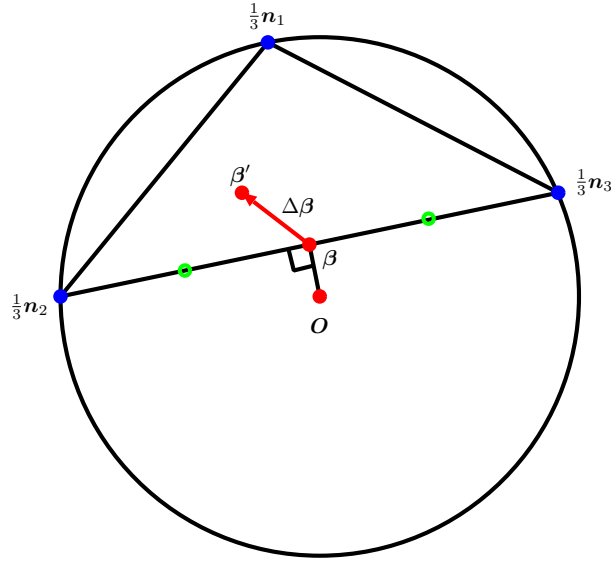


図 5.7: ベクトル  $\beta$  の終点から  $\Delta\beta$  だけずらしたベクトル  $\beta'$  の終点 (2)

仮定から, ベクトル  $\beta$  と三角形の各頂点との距離とベクトル  $\beta'$  と三角形の各頂点との距離には次のような関係が成り立つはずである.

$$\begin{aligned} \left| \beta - \frac{1}{3}n_1 \right| &> \left| \beta' - \frac{1}{3}n_1 \right|, \\ \left| \beta - \frac{1}{3}n_2 \right| &> \left| \beta' - \frac{1}{3}n_2 \right|, \\ \left| \beta - \frac{1}{3}n_3 \right| &> \left| \beta' - \frac{1}{3}n_3 \right|. \end{aligned}$$

しかしながら, この関係は外心が外周上を含む三角形の内部に存在する場合と同様の議論で矛盾することがわかる. それゆえ, 最初の仮定であるベクトル  $\beta$  の終点と三角形の各頂点との距離よりも各頂点との距離がすべて小さくなるような点が存在するということが矛盾していることになる. したがって, 最適なベクトル  $\beta$  は (5.39) 式で与えられることが示せた.

今, 最適なベクトル  $\beta$  は (5.39) 式で与えられることと (5.40) 式で与えられた関係から, 上限  $d$  の最小値は次のように与えられる.

$$d_{\min} = \alpha = \frac{1}{3} \left( 1 + \frac{|n_2 - n_3|}{2} \right). \quad (5.41)$$



(5.33) 式で与えられる上限  $d$  を達成する POVM を構成する. 今, 考えている (5.38a) 式を満たす場合では, 与えられた状態が  $\rho_1$  であると同定することを意味する POVM 要素  $E_1$  は  $E_1 = 0$  で与えられる. それは次のように示される. まず, POVM 要素  $E_1$  に対する実現可能条件は  $E_1 Y_1 = 0$  に書き換えられ,  $Y_1$  は次のように与えられる.

$$Y_1 = \frac{1}{12} [|n_2 - n_3| - (2n_1 - n_2 - n_3) \cdot \sigma].$$

この  $Y_1$  の固有値は簡単に得られ, 得られた 2 つの固有値がゼロではないことがわかる. それゆえ,  $\text{rank}(Y_1) = 2$  であることは明らかである. これは POVM 要素  $E_1$  のランクが 0 であることを意味する. したがって,  $E_1 = 0$  が与えられる.

さらに, POVM 要素  $E_2, E_3$  は (5.5) 式で与えられた実現可能条件から, それぞれ次のような形式で与えられる.

$$E_2 = C_2 \frac{1 + m \cdot \sigma}{2}, \quad E_3 = C_3 \frac{1 - m \cdot \sigma}{2},$$

ここで, ベクトル  $m$  は次のように定義された単位ベクトルである.

$$m \equiv \frac{n_2 - n_3}{|n_2 - n_3|}.$$

(5.2a), (5.2b) 式を満たすように係数  $C_2, C_3$  を決定する. (5.2b) 式で与えられる完全性関係から,  $C_2, C_3$  に対する次のような 2 つの関係が得られる.

$$\frac{1}{2} (C_2 + C_3) = 1, \quad (5.42)$$

$$C_2 m - C_3 m = 0. \quad (5.43)$$

この 2 つの関係式から,  $C_2 = C_3 = 1$  であることは明らかである. さらに,  $C_2 > 0$ ,  $C_3 > 0$  であることから, (5.2a) 式も満たされる.

以上から, (5.33) 式で与えられる上限  $d$  を達成する POVM が構成できた. そして, 最大識別成功確率は次のように与えられる.

$$p_{\max} = \frac{1}{3} \left( 1 + \frac{|n_2 - n_3|}{2} \right). \quad (5.44)$$

上の結果は (5.38a) 式を満たす場合を仮定して得られた. (5.38b) 式を満たす場合, (5.38c) 式を満たす場合を仮定しても, 同様の議論で最大識別成功確率が得られる.

### 5.3.3 例

次のような Bloch ベクトル  $n_1, n_2, n_3$  で定義される状態の集合を考える.

$$n_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad n_2 = \begin{pmatrix} \cos \varphi_2 \\ \sin \varphi_2 \\ 0 \end{pmatrix}, \quad n_3 = \begin{pmatrix} \cos \varphi_3 \sin \theta_3 \\ \sin \varphi_3 \sin \theta_3 \\ \cos \theta_3 \end{pmatrix}.$$

1 つめの例として, 図 5.8 では, それぞれ  $\varphi_2 = \pi/3$ ,  $\varphi_3 = \pi/6$  に固定した場合の  $\text{tr}[E_i]$  と最大識別成功確率  $p_{\max}$  を  $\theta_3$  の関数として表示している.  $\theta_3$  を 0 から  $2\pi$  まで変化させていくと, 最適な解のタイプが変化する. この例では, 3 つのベクトル  $n_1, n_2, n_3$  の終点がなす三角形は常に二等辺三角形であるが,  $\theta_3$  が大きくなるにつれて, 三角形が徐々につぶれていき,  $\theta_3 = 1.1(\text{rad})$  付近でベクトル  $n_3$  周りのなす角が鋭角から鈍角になり, 最適な解のタイプが変化する. そのとき,  $\text{tr}[E_i]$  のプロットを見ても明らかなように, POVM 要素  $E_3$  は 0 となってしまう. これは与えられた状態が  $\rho_3$  であるという推定をしない方が最適であることを意味する. さらに,  $\theta_3$  が大きくなると, 次は,  $\theta_3 = 2.1(\text{rad})$  付近でベクトル  $n_3$  周りのなす角が鈍角から鋭角になり, 最適な解のタイプも元に戻る.

また, 最大識別成功確率  $p_{\max}$  は  $\theta_3 = 4.7(\text{rad})$  付近で最大値  $2/3$  となる. そのとき, 3 つのベクトル  $n_1, n_2, n_3$  は同一平面上にあり, 外接円の半径  $R$  がちょうど 3 つのベクトルの長さ  $1/3$  と一致する. さらに,  $\theta_3$  が  $1.1(\text{rad})$  付近から  $2.1(\text{rad})$  付近までの範囲にあるとき, 最大識別成功確率  $p_{\max}$  は一定である. それは 3 つのベクトル  $n_1, n_2, n_3$  の終点がなす三角形は鈍角三角形であり, (5.38c) 式を満たす場合である. このような場合, 最大識別成功確率  $p_{\max}$  は次のように与えられる.

$$\begin{aligned} p_{\max} &= \frac{1}{3} \left( 1 + \frac{|n_1 - n_2|}{2} \right) = \frac{1}{3} \left( 1 + \frac{1}{2} \sqrt{(1 - \cos \varphi_2)^2 + (-\sin \varphi_2)^2} \right) \\ &= \frac{1}{3} \left( 1 + \sqrt{\frac{1 - \cos \varphi_2}{2}} \right). \end{aligned}$$

$p_{\max}$  が  $\theta_3$  に依らないことは明らかである. さらに, これはベクトル  $n_1$  とベクトル  $n_2$  間の距離が  $\theta_3$  に依らず, 一定であることも意味する. したがって,  $p_{\max}$  はこの範囲では一定である.

2 つめの例として, 図 5.9 では, それぞれ  $\varphi_2 = \pi/6$ ,  $\varphi_3 = \pi/3$  に固定した場合の  $\text{tr}[E_i]$  と最大識別成功確率  $p_{\max}$  を  $\theta_3$  の関数としてプロットしたものである. この例においても,  $\theta_3$  を 0 から  $2\pi$  まで変化させていくと, 最適な解のタイプが変化する. まず,  $\theta_3 = 0.3(\text{rad})$  付近でベクトル  $n_2$  周りのなす角が鋭角から鈍角になり, 最適な解のタイプが変化する. そのとき, (5.38b) 式を満たし, POVM 要素  $E_2$  は 0 となる. これは与えられた状態が  $\rho_2$  であると推定しないことを意味する. また,  $\theta_3 = 2.7(\text{rad})$  付近で 3 つの POVM 要素  $E_1, E_2, E_3$  が 0 でない解のタイプに変化する. さらに,  $\theta_3$  を大きくすると, 今度は  $\theta_3 = 3.6(\text{rad})$  付近でベクトル  $n_1$  周りのなす角が鋭角から鈍角になる. すなわち, (5.38a) 式を満たす場合である. そのとき, POVM 要素  $E_1$  は 0 となるような解のタイプに変化する. そして,  $\theta_3 = 5.9(\text{rad})$  付近で 3 つの POVM 要素  $E_1, E_2, E_3$  が 0 でない解のタイプに戻る.

また, この例では, 1 つめの例とは違い, 最大識別成功確率  $p_{\max}$  が一定となるような範囲はない. それはこの例では先ほどの例とは違い, 最大識別成功確率  $p_{\max}$  は常に  $\theta_3$  によって変化するからである. それゆえ, 最大識別成功確率  $p_{\max}$  に関するベクトル  $n_1$  とベクトル  $n_3$  間の距離もベクトル  $n_2$  とベクトル  $n_3$  間の距離も  $\theta_3$  によって変化する事がわかる.

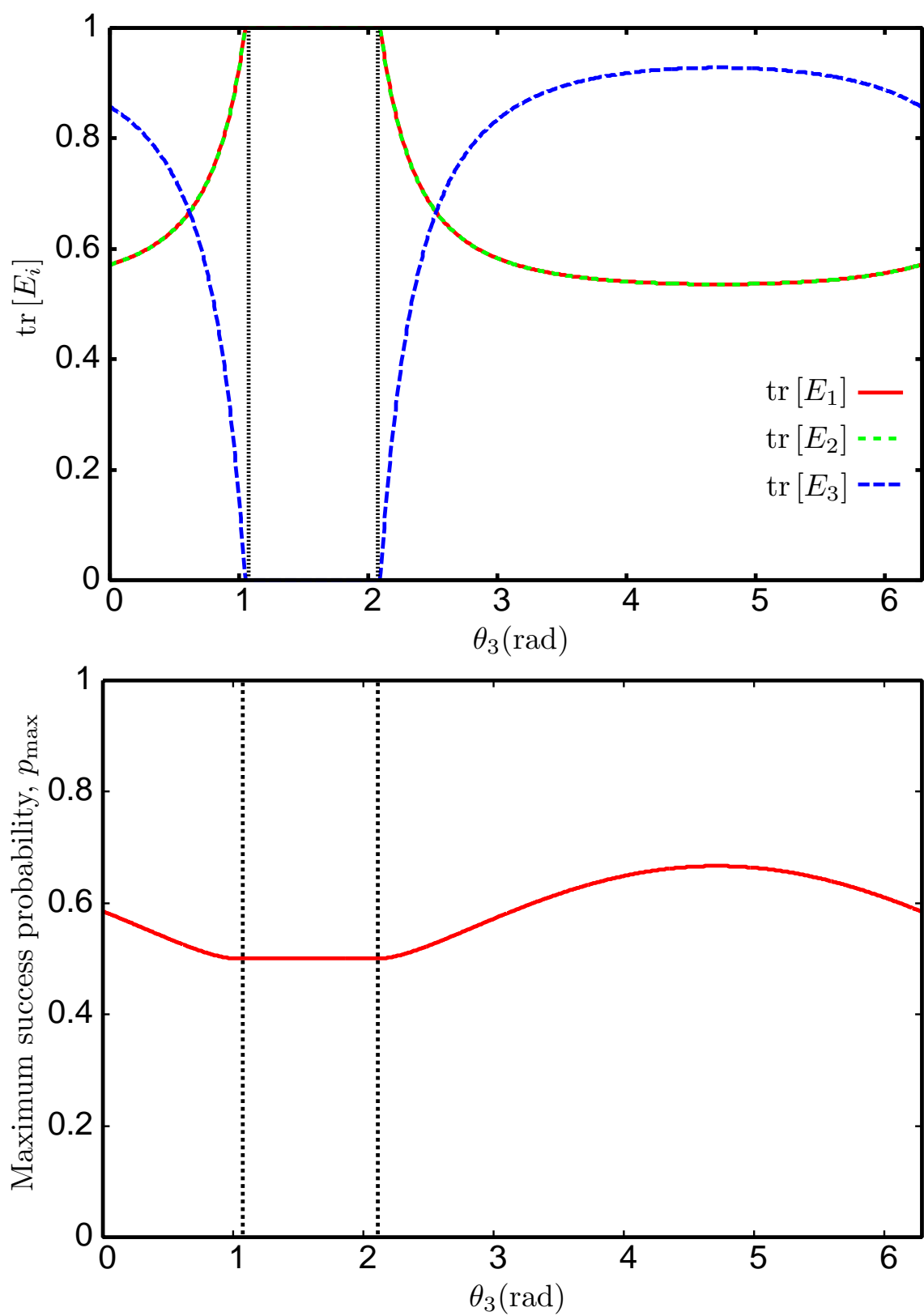


図 5.8:  $\theta_3$  に対する  $\text{tr}[E_i]$ (上部) と最大識別成功確率  $p_{\max}$ (下部) (1)

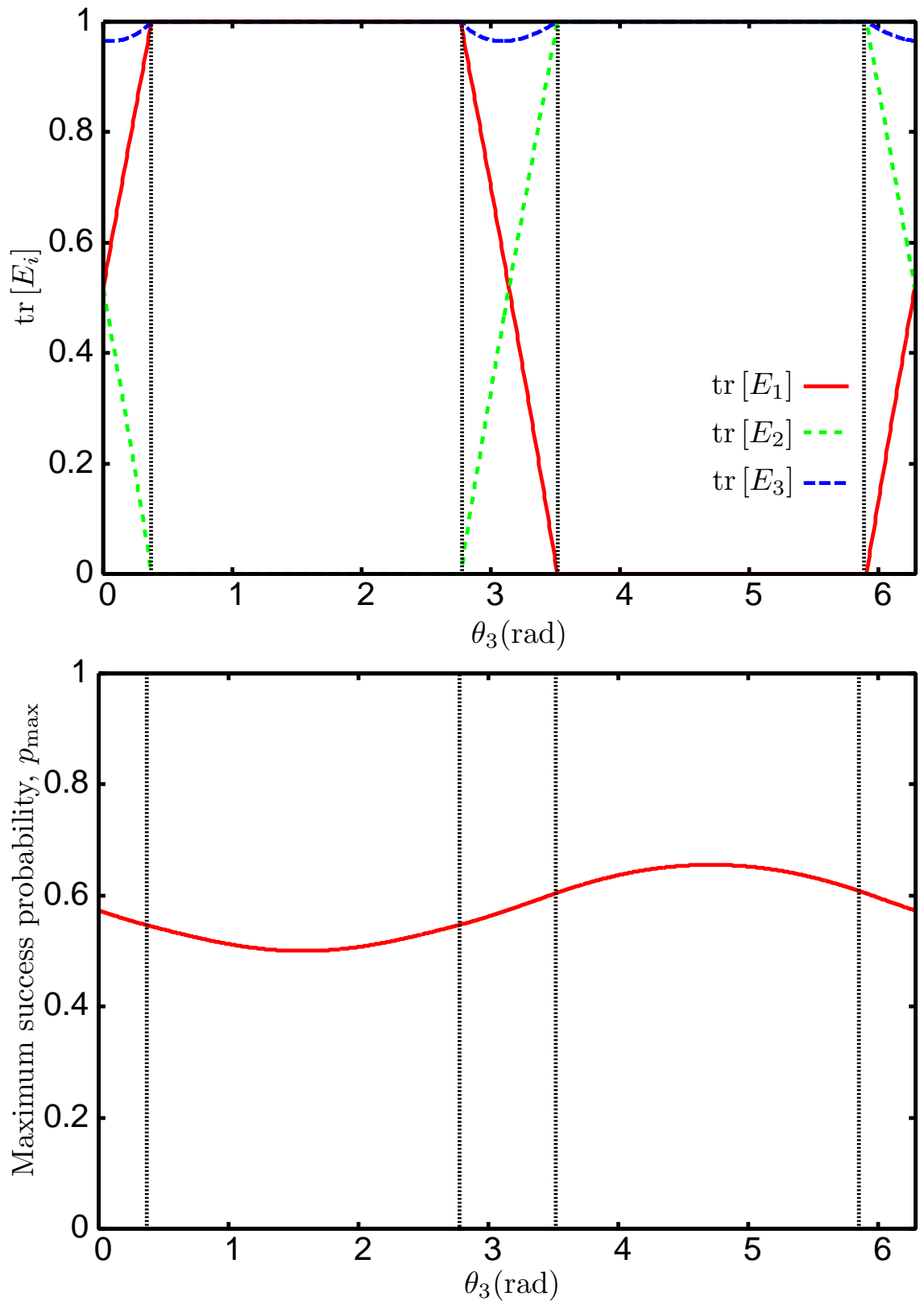


図 5.9:  $\theta_3$  に対する  $\text{tr}[E_i]$ (上部) と最大識別成功確率  $p_{\max}$ (下部) (2)

## 5.4 一般の生起確率を持つ qubit の 3 つの純粋状態の場合

本節では, 一般の生起確率  $\eta_i$  を持つ qubit の 3 つの純粋状態  $\rho_i = |\phi_i\rangle\langle\phi_i|$  の minimum-error discrimination を考える. しかしながら, この場合では, まだ完全に解析解が得られていない. それゆえ, 現在までにわかっていることを以下にまとめる.

Bloch ベクトル表示を用いて, 双対問題は次のように書き換えられる.

minimize :

$$d = \alpha, \quad (5.45a)$$

subject to :

$$\alpha \geq \eta_1 + |\beta - \eta_1 \mathbf{n}_1|, \quad (5.45b)$$

$$\alpha \geq \eta_2 + |\beta - \eta_2 \mathbf{n}_2|, \quad (5.45c)$$

$$\alpha \geq \eta_3 + |\beta - \eta_3 \mathbf{n}_3|. \quad (5.45d)$$

一般の生起確率を持つ 2 つの純粋状態の場合, 最適なベクトル  $\beta$  の終点はベクトル  $\eta_1 \mathbf{n}_1, \eta_2 \mathbf{n}_2$  それぞれの終点を結ぶ直線上にあった. また, 生起確率が等しい qubit の 3 つの純粋状態の場合, 最適なベクトル  $\beta$  の終点はベクトル  $\mathbf{n}_1/3, \mathbf{n}_2/3, \mathbf{n}_3/3$  それぞれの終点がなす三角形上にあった. それゆえ, 一般の生起確率を持つ qubit の 3 つの純粋状態の場合でも同様に, 最適なベクトル  $\beta$  の終点は 3 つのベクトル  $\eta_1 \mathbf{n}_1, \eta_2 \mathbf{n}_2, \eta_3 \mathbf{n}_3$  それぞれの終点がなす三角形上に存在すると考えられる. この仮定が正しいことは次のようにして示すことができる.

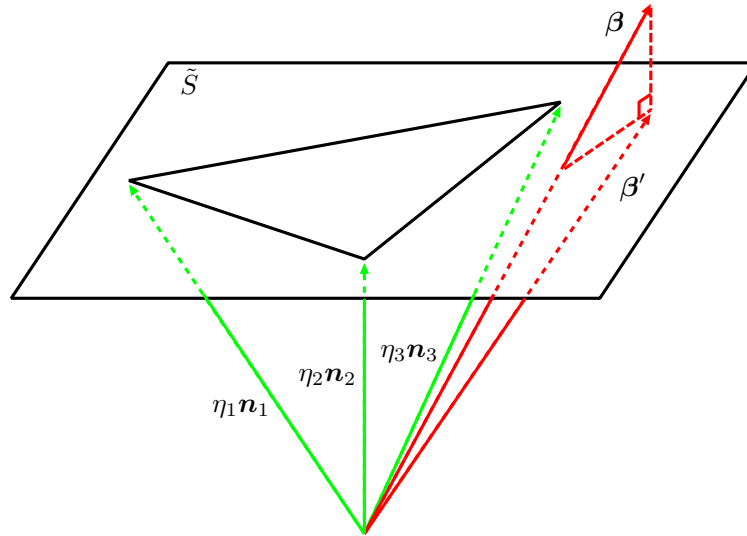


図 5.10: 最適なベクトル  $\beta(1)$

まず, 最適なベクトル  $\beta$  の終点は 3 つのベクトル  $\eta_1 \mathbf{n}_1, \eta_2 \mathbf{n}_2, \eta_3 \mathbf{n}_3$  それぞれの終点がなす三角形を含む平面上にあることを示す. 3 つのベクトル  $\eta_1 \mathbf{n}_1, \eta_2 \mathbf{n}_2, \eta_3 \mathbf{n}_3$  それぞれの終点がなす三角形を含む平面を  $\tilde{S}$  とし, ベクトル  $\beta$  の終点はその平面  $\tilde{S}$  上にはないとする. 図 5.10 のようにベクトル  $\beta$  の終点から平面  $\tilde{S}$  に対して垂線を下ろし, その垂

線と平面  $\tilde{S}$  の交点が終点であるベクトル  $\beta'$  があったとする. 今, ベクトル  $\beta, \beta'$  それぞれの終点と三角形の頂点との距離に注目すると, 次のような関係が成り立つことは明らかである.

$$\begin{aligned} |\beta - \eta_1 \mathbf{n}_1| &> |\beta' - \eta_1 \mathbf{n}_1|, \\ |\beta - \eta_2 \mathbf{n}_2| &> |\beta' - \eta_2 \mathbf{n}_2|, \\ |\beta - \eta_3 \mathbf{n}_3| &> |\beta' - \eta_3 \mathbf{n}_3|. \end{aligned}$$

この関係はベクトル  $\beta$  よりもベクトル  $\beta'$  の方がより小さい  $d$  を与えることを意味する. それゆえ, 最適な  $\beta$  の終点は平面  $\tilde{S}$  上にあることがわかる.

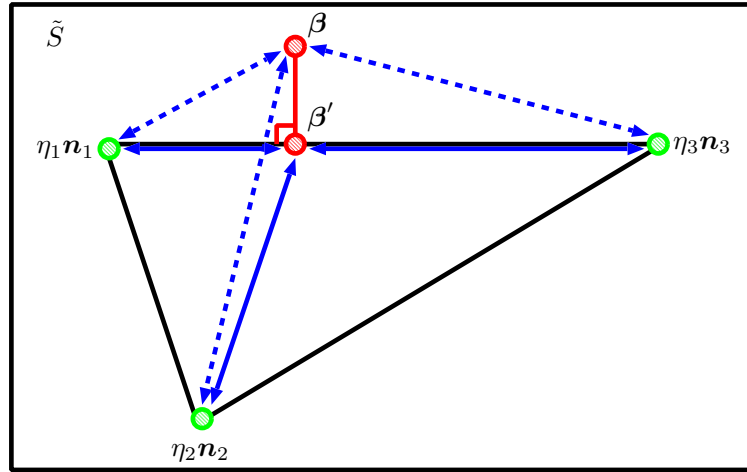


図 5.11: 最適なベクトル  $\beta(2)$

次に, 最適なベクトル  $\beta$  の終点は3つのベクトル  $\eta_1 \mathbf{n}_1, \eta_2 \mathbf{n}_2, \eta_3 \mathbf{n}_3$  それぞれの終点がなす三角形上にあることを示す. ベクトル  $\beta$  の終点は平面  $\tilde{S}$  上にはあるが, 3つのベクトル  $\eta_1 \mathbf{n}_1, \eta_2 \mathbf{n}_2, \eta_3 \mathbf{n}_3$  それぞれの終点がなす三角形上にはないとする. 図 5.11 は平面  $\tilde{S}$  を真上から見た図であるが, この図のようにベクトル  $\beta$  の終点から一番近い三角形の辺に対して垂線を下ろし, その辺との交点が終点であるベクトル  $\beta'$  があったとする. そのとき, ベクトル  $\beta, \beta'$  それぞれの終点と三角形の頂点との距離に注目すると, 次のような関係が成り立つ.

$$\begin{aligned} |\beta - \eta_1 \mathbf{n}_1| &> |\beta' - \eta_1 \mathbf{n}_1|, \\ |\beta - \eta_2 \mathbf{n}_2| &> |\beta' - \eta_2 \mathbf{n}_2|, \\ |\beta - \eta_3 \mathbf{n}_3| &> |\beta' - \eta_3 \mathbf{n}_3|. \end{aligned}$$

この関係はベクトル  $\beta$  よりもベクトル  $\beta'$  の方がより小さい  $d$  を与えることを意味する. それゆえ, 最適なベクトル  $\beta$  の終点は三角形上にあることがわかる. ただし, 図 5.12 のように, 一番近い三角形の辺に対して垂線が下ろせない場合がある. このような場合, 上での議論と同様にして, 三角形の頂点にベクトル  $\beta$  の終点をとればよいことがわかる.

以上から, 最適なベクトル  $\beta$  の終点は3つのベクトル  $\eta_1 \mathbf{n}_1, \eta_2 \mathbf{n}_2, \eta_3 \mathbf{n}_3$  それぞれの終点がなす三角形上に存在することが示された.

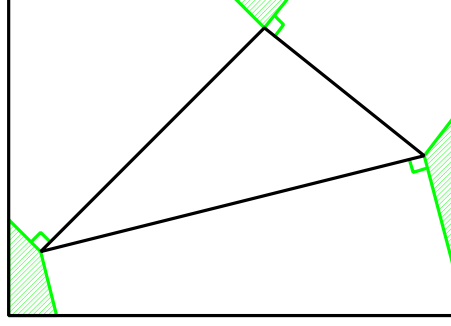


図 5.12: 一番近い辺に対して垂線が下ろせない領域

等しい生起確率を持つ qubit の 3 つの純粋状態の場合, 識別される状態の 3 つの Bloch ベクトル  $\eta_1 \mathbf{n}_1, \eta_2 \mathbf{n}_2, \eta_3 \mathbf{n}_3$  の終点がなす三角形の外心にベクトル  $\beta$  の終点が存在するとき, 最適であった. それゆえ, 一般の生起確率を持つ qubit の 3 つの純粋状態の場合では, (5.45b), (5.45c), (5.45d) 式で与えられた不等式において, 等号が成り立つ場合を仮定する.

$$\alpha = \eta_1 + |\beta - \eta_1 \mathbf{n}_1| = \eta_2 + |\beta - \eta_2 \mathbf{n}_2| = \eta_3 + |\beta - \eta_3 \mathbf{n}_3|. \quad (5.46)$$

また, 最適な  $\beta$  の終点が 3 つの Bloch ベクトル  $\eta_1 \mathbf{n}_1, \eta_2 \mathbf{n}_2, \eta_3 \mathbf{n}_3$  の終点がなす三角形上にあることはわかっている. もし, (5.46) 式を満たす  $\beta$  の終点が三角形上に存在するならば, その  $\beta$  は最適であると言える. それは次のようにして示すことができる.

今, (5.46) 式を満たすベクトル  $\beta$  の終点が 3 つのベクトル  $\eta_1 \mathbf{n}_1, \eta_2 \mathbf{n}_2, \eta_3 \mathbf{n}_3$  の終点がなす三角形上に存在するとする. その  $\beta$  の終点から  $\Delta\beta$  だけずらした点を終点とするベクトル  $\beta'$  を定義する. もし,  $\beta'$  が最適であるならば, 次のような 3 つの不等式を同時に満たすはずである.

$$\begin{aligned} \eta_1 + |\beta - \eta_1 \mathbf{n}_1| &> \eta_1 + |\beta' - \eta_1 \mathbf{n}_1|, \\ \eta_2 + |\beta - \eta_2 \mathbf{n}_2| &> \eta_2 + |\beta' - \eta_2 \mathbf{n}_2|, \\ \eta_3 + |\beta - \eta_3 \mathbf{n}_3| &> \eta_3 + |\beta' - \eta_3 \mathbf{n}_3|. \end{aligned}$$

しかしながら, そのような  $\beta'$  は存在しない. そして, それは 5.3.1 節の議論と同様にして証明される. まず, 3 つの不等式は次のように書き換えられる.

$$\begin{aligned} |\beta - \eta_1 \mathbf{n}_1| &> |\beta - \eta_1 \mathbf{n}_1 + \Delta\beta|, \\ |\beta - \eta_2 \mathbf{n}_2| &> |\beta - \eta_2 \mathbf{n}_2 + \Delta\beta|, \\ |\beta - \eta_3 \mathbf{n}_3| &> |\beta - \eta_3 \mathbf{n}_3 + \Delta\beta|. \end{aligned}$$

これら 3 つの不等式に対して, (5.25) 式で与えられた不等式を適用すると, 次のような不等式が得られる.

$$\begin{aligned} 0 &> (\beta - \eta_1 \mathbf{n}_1) \cdot \Delta\beta, \\ 0 &> (\beta - \eta_2 \mathbf{n}_2) \cdot \Delta\beta, \\ 0 &> (\beta - \eta_3 \mathbf{n}_3) \cdot \Delta\beta. \end{aligned}$$

これら 3 つの不等式にそれぞれ任意の実数  $x, y, z$  を掛けて和をとると、次のような不等式が得られる。

$$0 > [(x + y + z) \beta - (x\eta_1 \mathbf{n}_1 + y\eta_2 \mathbf{n}_2 + z\eta_3 \mathbf{n}_3)] \cdot \Delta \beta.$$

今、ベクトル  $\beta$  の終点が 3 つのベクトル  $\eta_1 \mathbf{n}_1, \eta_2 \mathbf{n}_2, \eta_3 \mathbf{n}_3$  の終点がなす三角形上に存在することから、 $\beta$  は次のように与えられる。

$$\beta = x\eta_1 \mathbf{n}_1 + y\eta_2 \mathbf{n}_2 + z\eta_3 \mathbf{n}_3,$$

ここで、 $x, y, z$  は  $x \geq 0, y \geq 0, z \geq 0$  であり、 $x + y + z = 1$  を満たす実数である。したがって、上の不等式は次のような不等式に書き換えられる。

$$0 > 0 \cdot \Delta \beta.$$

この不等式は明らかに矛盾している。つまり、最初の 3 つの不等式を同時に満たすようなベクトル  $\beta'$  は存在しないことが証明された。したがって、(5.46) 式を満たすベクトル  $\beta$  の終点が 3 つのベクトル  $\eta_1 \mathbf{n}_1, \eta_2 \mathbf{n}_2, \eta_3 \mathbf{n}_3$  の終点がなす三角形上に存在するならば、その  $\beta$  が最適であることが示せた。

以上から、(5.46) 式を満たすようなベクトル  $\beta$  を決定する。まず、(5.46) 式から次のような 3 つの関係式が得られる。

$$\begin{aligned} \eta_1 + |\beta - \eta_1 \mathbf{n}_1| &= \eta_2 + |\beta - \eta_2 \mathbf{n}_2|, \\ \eta_2 + |\beta - \eta_2 \mathbf{n}_2| &= \eta_3 + |\beta - \eta_3 \mathbf{n}_3|, \\ \eta_3 + |\beta - \eta_3 \mathbf{n}_3| &= \eta_1 + |\beta - \eta_1 \mathbf{n}_1|. \end{aligned}$$

これらの 3 式の両辺を 2 乗して整理すると、それぞれ

$$\begin{aligned} \eta_1 (\eta_1 + |\beta - \eta_1 \mathbf{n}_1|) - \eta_2 (\eta_2 + |\beta - \eta_2 \mathbf{n}_2|) - (\eta_1 \mathbf{n}_1 - \eta_2 \mathbf{n}_2) \cdot \beta &= 0, \\ \eta_2 (\eta_2 + |\beta - \eta_2 \mathbf{n}_2|) - \eta_3 (\eta_3 + |\beta - \eta_3 \mathbf{n}_3|) - (\eta_2 \mathbf{n}_2 - \eta_3 \mathbf{n}_3) \cdot \beta &= 0, \\ \eta_3 (\eta_3 + |\beta - \eta_3 \mathbf{n}_3|) - \eta_1 (\eta_1 + |\beta - \eta_1 \mathbf{n}_1|) - (\eta_3 \mathbf{n}_3 - \eta_1 \mathbf{n}_1) \cdot \beta &= 0, \end{aligned}$$

となる。さらに、(5.46) 式を用いると、これらの 3 式は次のように書き換えられる。

$$(\eta_1 - \eta_2) \alpha + \mathbf{c} \cdot \beta = 0, \quad (5.47)$$

$$(\eta_2 - \eta_3) \alpha + \mathbf{a} \cdot \beta = 0, \quad (5.48)$$

$$(\eta_3 - \eta_1) \alpha + \mathbf{b} \cdot \beta = 0, \quad (5.49)$$

ここで、次のように定義された 3 つのベクトル  $\mathbf{a}, \mathbf{b}, \mathbf{c}$  を導入した。

$$\mathbf{a} \equiv \eta_3 \mathbf{n}_3 - \eta_2 \mathbf{n}_2, \quad (5.50)$$

$$\mathbf{b} \equiv \eta_1 \mathbf{n}_1 - \eta_3 \mathbf{n}_3, \quad (5.51)$$

$$\mathbf{c} \equiv \eta_2 \mathbf{n}_2 - \eta_1 \mathbf{n}_1. \quad (5.52)$$



ただし, (5.47), (5.48), (5.49) 式で与えられる 3 つの関係式のうちの 1 つの式はその他の 2 式から導出することができる. つまり, これら 3 つの関係式のうち, 2 つの関係式を満たせば, 残り 1 つの関係式も自動的に満たされる.

今, ベクトル  $\beta$  の終点は 3 つのベクトル  $\eta_1 \mathbf{n}_1, \eta_2 \mathbf{n}_2, \eta_3 \mathbf{n}_3$  それぞれの終点がなす三角形上に存在することから, ベクトル  $\beta$  は次のように与えられる.

$$\beta = s\eta_1 \mathbf{n}_1 + t\eta_2 \mathbf{n}_2 + u\eta_3 \mathbf{n}_3,$$

ここで,  $s, t, u$  は  $s \geq 0, t \geq 0, u \geq 0$  であり,  $s + t + u = 1$  を満たす実数である. また,  $s + t + u = 1$  を満たすことから, ベクトル  $\beta$  は次のように書き換えることができる.

$$\beta = \eta_1 \mathbf{n}_1 + t\mathbf{c} - u\mathbf{b}.$$

このベクトル  $\beta$  を (5.47), (5.49) 式それぞれに代入すると, 次のような  $t, u$  に関する連立方程式が得られる.

$$\begin{aligned} |\mathbf{c}|^2 t - (\mathbf{b} \cdot \mathbf{c}) u &= (\eta_2 - \eta_1) \alpha - \eta_1 \mathbf{n}_1 \cdot \mathbf{c}, \\ (\mathbf{b} \cdot \mathbf{c}) t - |\mathbf{b}|^2 u &= (\eta_1 - \eta_3) \alpha - \eta_1 \mathbf{n}_1 \cdot \mathbf{b}. \end{aligned}$$

この連立方程式を解くことで,  $t, u$  は次のように与えられる.

$$\begin{aligned} t &= \left( \frac{\alpha(\eta_1 \mathbf{a} + \eta_2 \mathbf{b} + \eta_3 \mathbf{c}) - [(\eta_1 \mathbf{n}_1 \cdot \mathbf{c}) \mathbf{b} - (\eta_1 \mathbf{n}_1 \cdot \mathbf{b}) \mathbf{c}]}{|\mathbf{b}|^2 |\mathbf{c}|^2 - (\mathbf{b} \cdot \mathbf{c})^2} \right) \cdot \mathbf{b}, \\ u &= \left( \frac{\alpha(\eta_1 \mathbf{a} + \eta_2 \mathbf{b} + \eta_3 \mathbf{c}) - [(\eta_1 \mathbf{n}_1 \cdot \mathbf{c}) \mathbf{b} - (\eta_1 \mathbf{n}_1 \cdot \mathbf{b}) \mathbf{c}]}{|\mathbf{b}|^2 |\mathbf{c}|^2 - (\mathbf{b} \cdot \mathbf{c})^2} \right) \cdot \mathbf{c}. \end{aligned}$$

これらの  $t, u$  は (5.50), (5.51), (5.52) 式や  $\mathbf{a} + \mathbf{b} + \mathbf{c} = 0$  であることを用いて, 次のように書き換えることができる.

$$\begin{aligned} t &= \frac{4S^2 + \alpha(\eta_1 \mathbf{a} + \eta_2 \mathbf{b} + \eta_3 \mathbf{c}) \cdot \mathbf{b} - [(\eta_2 \mathbf{n}_2 \cdot \mathbf{a}) \mathbf{c} - (\eta_2 \mathbf{n}_2 \cdot \mathbf{c}) \mathbf{a}] \cdot \mathbf{b}}{4S^2}, \\ u &= \frac{4S^2 + \alpha(\eta_1 \mathbf{a} + \eta_2 \mathbf{b} + \eta_3 \mathbf{c}) \cdot \mathbf{c} - [(\eta_3 \mathbf{n}_3 \cdot \mathbf{b}) \mathbf{a} - (\eta_3 \mathbf{n}_3 \cdot \mathbf{a}) \mathbf{b}] \cdot \mathbf{c}}{4S^2}, \end{aligned}$$

ここで,  $S$  は 3 つのベクトル  $\eta_1 \mathbf{n}_1, \eta_2 \mathbf{n}_2, \eta_3 \mathbf{n}_3$  の終点がなす三角形の面積である. また,  $|\mathbf{b}|^2 |\mathbf{c}|^2 - (\mathbf{b} \cdot \mathbf{c})^2 = 4S^2$  となることは付録 B を参照した. さらに,  $s + t + u = 1$  を満たすことから,  $s$  は次のように与えられる.

$$\begin{aligned} s &= 1 - t - u \\ &= \frac{4S^2 + \alpha(\eta_1 \mathbf{a} + \eta_2 \mathbf{b} + \eta_3 \mathbf{c}) \cdot \mathbf{a} - [(\eta_1 \mathbf{n}_1 \cdot \mathbf{c}) \mathbf{b} - (\eta_1 \mathbf{n}_1 \cdot \mathbf{b}) \mathbf{c}] \cdot \mathbf{a}}{4S^2}. \end{aligned}$$

今,  $s$  のすべての項をベクトル  $\mathbf{a}, \mathbf{b}, \mathbf{c}$  で書くために,  $\eta_1 \mathbf{n}_1 \cdot \mathbf{c}$  と  $\eta_1 \mathbf{n}_1 \cdot \mathbf{b}$  に対して, 次のような操作を行う.

$$\begin{aligned} \eta_1 \mathbf{n}_1 \cdot \mathbf{c} &= \left( \frac{\eta_2 \mathbf{n}_2 + \eta_1 \mathbf{n}_1}{2} - \frac{\eta_2 \mathbf{n}_2 - \eta_1 \mathbf{n}_1}{2} \right) \cdot \mathbf{c} \\ &= \frac{1}{2} (\eta_2^2 - \eta_1^2 - |\mathbf{c}|^2), \end{aligned} \tag{5.53a}$$

$$\begin{aligned} \eta_1 \mathbf{n}_1 \cdot \mathbf{b} &= \left( \frac{\eta_1 \mathbf{n}_1 + \eta_3 \mathbf{n}_3}{2} + \frac{\eta_1 \mathbf{n}_1 - \eta_3 \mathbf{n}_3}{2} \right) \cdot \mathbf{b} \\ &= \frac{1}{2} (\eta_1^2 - \eta_3^2 - |\mathbf{b}|^2). \end{aligned} \tag{5.53b}$$

$t$  の  $\eta_2 \mathbf{n}_2 \cdot \mathbf{a}$  と  $\eta_2 \mathbf{n}_2 \cdot \mathbf{c}$ ,  $u$  の  $\eta_3 \mathbf{n}_3 \cdot \mathbf{b}$  と  $\eta_3 \mathbf{n}_3 \cdot \mathbf{a}$  に対しても同様の操作を行うと,  $s, t, u$  はそれぞれ次のように書き換えられる.

$$\begin{aligned} s &= \frac{8S^2 + 2\alpha(\eta_1 \mathbf{a} + \eta_2 \mathbf{b} + \eta_3 \mathbf{c}) \cdot \mathbf{a} - (\eta_1^2 \mathbf{a} + \eta_2^2 \mathbf{b} + \eta_3^2 \mathbf{c}) \cdot \mathbf{a} + |\mathbf{b}|^2 (\mathbf{c} \cdot \mathbf{a}) + |\mathbf{c}|^2 (\mathbf{a} \cdot \mathbf{b})}{8S^2}, \\ t &= \frac{8S^2 + 2\alpha(\eta_1 \mathbf{a} + \eta_2 \mathbf{b} + \eta_3 \mathbf{c}) \cdot \mathbf{b} - (\eta_1^2 \mathbf{a} + \eta_2^2 \mathbf{b} + \eta_3^2 \mathbf{c}) \cdot \mathbf{b} + |\mathbf{a}|^2 (\mathbf{b} \cdot \mathbf{c}) + |\mathbf{c}|^2 (\mathbf{a} \cdot \mathbf{b})}{8S^2}, \\ u &= \frac{8S^2 + 2\alpha(\eta_1 \mathbf{a} + \eta_2 \mathbf{b} + \eta_3 \mathbf{c}) \cdot \mathbf{c} - (\eta_1^2 \mathbf{a} + \eta_2^2 \mathbf{b} + \eta_3^2 \mathbf{c}) \cdot \mathbf{c} + |\mathbf{a}|^2 (\mathbf{b} \cdot \mathbf{c}) + |\mathbf{b}|^2 (\mathbf{c} \cdot \mathbf{a})}{8S^2}. \end{aligned}$$

また,  $s + t + u = 1$  は次のような恒等式が成り立つことを意味する.

$$-\frac{1}{8S^2} [|\mathbf{a}|^2 (\mathbf{b} \cdot \mathbf{c}) + |\mathbf{b}|^2 (\mathbf{c} \cdot \mathbf{a}) + |\mathbf{c}|^2 (\mathbf{a} \cdot \mathbf{b})] = 1. \quad (5.54)$$

この恒等式を用いて,  $s, t, u$  はそれぞれ次のように書き換えられる.

$$s = \frac{2\alpha(\mathbf{D} \cdot \mathbf{a}) - [\mathbf{D}' \cdot \mathbf{a} + |\mathbf{a}|^2 (\mathbf{b} \cdot \mathbf{c})]}{8S^2}, \quad (5.55)$$

$$t = \frac{2\alpha(\mathbf{D} \cdot \mathbf{b}) - [\mathbf{D}' \cdot \mathbf{b} + |\mathbf{b}|^2 (\mathbf{c} \cdot \mathbf{a})]}{8S^2}, \quad (5.56)$$

$$u = \frac{2\alpha(\mathbf{D} \cdot \mathbf{c}) - [\mathbf{D}' \cdot \mathbf{c} + |\mathbf{c}|^2 (\mathbf{a} \cdot \mathbf{b})]}{8S^2}, \quad (5.57)$$

ここで,  $\mathbf{D}, \mathbf{D}'$  は次のように定義される.

$$\mathbf{D} \equiv \eta_1 \mathbf{a} + \eta_2 \mathbf{b} + \eta_3 \mathbf{c}, \quad (5.58)$$

$$\mathbf{D}' \equiv \eta_1^2 \mathbf{a} + \eta_2^2 \mathbf{b} + \eta_3^2 \mathbf{c}. \quad (5.59)$$

上限  $d$  が最小となる  $\alpha$  を決定する. そして, それは次のような方法でなされる. (5.46) 式から, 次のような  $\alpha$  についての方程式が得られる.

$$\alpha - \eta_1 = |\boldsymbol{\beta} - \eta_1 \mathbf{n}_1|.$$

この方程式を両辺 2 乗すると

$$\alpha^2 - 2\eta_1 \alpha - \eta_1^2 = t\boldsymbol{\beta} \cdot \mathbf{c} - u\boldsymbol{\beta} \cdot \mathbf{b} - t(\eta_1 \mathbf{n}_1 \cdot \mathbf{c}) + u(\eta_1 \mathbf{n}_1 \cdot \mathbf{b}),$$

となる. ここで, 方程式の右辺は  $|\boldsymbol{\beta} - \eta_1 \mathbf{n}_1|^2 = (\boldsymbol{\beta} - \eta_1 \mathbf{n}_1) \cdot (t\mathbf{c} - u\mathbf{b})$  として, 計算した. さらに, この方程式は (5.47), (5.49), (5.53), (5.56), (5.57) 式を用いると, 次のような  $\alpha$  についての 2 次方程式に書き換えられる.

$$k\alpha^2 - l\alpha + m = 0,$$

ここで, 係数  $k, l, m$  は次のように与えられる.

$$\begin{aligned} k &= |\mathbf{D}|^2 - 4S^2, \\ l &= \mathbf{D} \cdot \mathbf{D}' + \eta_1 |\mathbf{a}|^2 (\mathbf{b} \cdot \mathbf{c}) + \eta_2 |\mathbf{b}|^2 (\mathbf{c} \cdot \mathbf{a}) + \eta_3 |\mathbf{c}|^2 (\mathbf{a} \cdot \mathbf{b}), \\ m &= \frac{1}{4} \left\{ |\mathbf{D}'|^2 + |\mathbf{a}|^2 |\mathbf{b}|^2 |\mathbf{c}|^2 + 2 [\eta_1^2 |\mathbf{a}|^2 (\mathbf{b} \cdot \mathbf{c}) + \eta_2^2 |\mathbf{b}|^2 (\mathbf{c} \cdot \mathbf{a}) + \eta_3^2 |\mathbf{c}|^2 (\mathbf{a} \cdot \mathbf{b})] \right\}. \end{aligned}$$

したがって, 2 次方程式の解の公式を用いると,  $\alpha$  は次のように得られる.

$$\alpha = \frac{l \pm \sqrt{l^2 - 4km}}{2k}. \quad (5.60)$$

問題は判別式  $l^2 - 4km$  が正かどうかである. もし, 判別式が負であるならば, 2 つの虚数根を持つことになり, この解は不適であることは明らかである. つまり, (5.46) 式で与えられた最初の仮定が間違っていたことになる. 一方で, 判別式が正であるならば, 得られた 2 つの実数根のうち, どちらが適するのかをチェックする必要がある.

しかしながら, 今のところ, 判別式はまだ計算できていない. 現在も継続して解析を行っているが, 計算が複雑で完全に解析解を得るに至っていない.

## 第6章 3つの純粋状態の unambiguous discrimination

お互いの内積が実数である3つの一般の純粋状態の unambiguous discrimination に対して、完全な解は閉じた解析的な形式で与えられる。この目的のために、まず、 $n$  個の線形独立な純粋状態の unambiguous discrimination でのいくつかの一般的な結果を証明する。また、解の一意性についても証明する。さらに、問題が  $(n - 1)$ -state problem に変換される条件を明確にする。お互いの内積が実数である3つの純粋状態に対する解を与えたあと、この方法を内積が複素数の場合に拡張する。そして、解析解が得られた内積が複素数である3つの純粋状態の集合について、紹介する。

### 6.1 一般論

#### 6.1.1 問題の定式化

状態は生起確率  $\eta_i$  を持つ  $n$  個の既知の純粋状態  $|\phi_i\rangle$  の集合から与えられたとする。また、 $n$  個の状態は線形独立であることと生起確率  $\eta_i$  は0でないことも仮定する。課題は与えられた状態が  $n$  個の状態の集合の中の1つであると明快に同定することである。すなわち、間違った同定は許されないが、結論の出ない結果(”わからない”)は許容される。

測定は POVM によって記述され、 $n + 1$  個の要素  $\{E_1, E_2, \dots, E_n, E_0\}$  から構成される。そして、それぞれの要素は状態  $|\phi_i\rangle$  によって張られた  $n$  次元空間  $V$  上の半正定値演算子である。測定結果が  $i$  ( $i = 1, \dots, n$ ) であるとき、与えられた状態は  $|\phi_i\rangle$  であると同定される。要素  $E_0$  は結論の出ない結果に対応する。そして、POVM は次のような完全性関係を満たす。

$$E_0 + \sum_{i=1}^n E_i = I_V. \quad (6.1)$$

Unambiguous discrimination では、識別に間違いは許されない。それゆえ、与えられた状態が  $|\phi_j\rangle$  かつ測定結果  $i$  を得る確率は0でなければならない。

$$\langle \phi_j | E_i | \phi_j \rangle = 0 \quad (i \neq j). \quad (6.2)$$

そして、それは半正定値演算子  $E_i$  の台集合が状態  $\{|\phi_j\rangle\}_{j(\neq i)}$  によって張られる  $n - 1$  次元部分空間と直交する補集合の1次元部分空間であることを要請する。したがって、POVM 要素  $E_i$  は次のような形式をとらなければならない [24]。

$$E_i = x_i |\tilde{\phi}_i\rangle\langle \tilde{\phi}_i|, \quad (6.3)$$

ここで,  $x_i$  は非負の定数である. そして,  $|\tilde{\phi}_i\rangle$  は  $j \neq i$  に関してどんな状態  $|\phi_j\rangle$  とも直交する状態である. 便宜のために, 状態  $|\tilde{\phi}_i\rangle$  を次のように規格化する.

$$\langle \tilde{\phi}_i | \phi_j \rangle = \delta_{ij}. \quad (6.4)$$

状態  $|\phi_i\rangle$  は線形独立であることから, 状態  $|\tilde{\phi}_i\rangle$  は次のように一意的に与えられる.

$$|\tilde{\phi}_i\rangle = \sum_{j=1}^n (N^{-1})_{ji} |\phi_j\rangle, \quad (6.5)$$

ここで,  $N$  は次のように定義される Gram 行列である.

$$N_{ij} \equiv \langle \phi_i | \phi_j \rangle.$$

もし, 与えられた状態が  $|\phi_i\rangle$  ならば, 係数  $x_i$  は与えられた状態がうまく同定されることを表す条件付き確率である. 識別成功確率  $p_o$  は  $x_i$  を用いて, 次のように与えられる.

$$p_o = \sum_{i=1}^n \eta_i \langle \phi_i | E_i | \phi_i \rangle = \sum_{i=1}^n \eta_i x_i. \quad (6.6)$$

今, POVM 要素  $E_0$  の半正定値性が係数  $x_i$  に対して課される条件について調べる. (6.1) 式で与えられた完全性関係によって,  $E_0$  の半正定値性は次のように表すことができる.

$$I_V - \sum_{i=1}^n x_i |\tilde{\phi}_i\rangle \langle \tilde{\phi}_i| \geq 0. \quad (6.7)$$

状態  $|\phi_i\rangle$  は線形独立であることから, この条件は次のように定義される  $n \times n$  行列  $M$  の半正定値性と等価である.

$$\begin{aligned} M_{ij} &= \langle \phi_i | \left( I_V - \sum_{k=1}^n x_k |\tilde{\phi}_k\rangle \langle \tilde{\phi}_k| \right) | \phi_j \rangle \\ &= N_{ij} - x_i \delta_{ij}. \end{aligned} \quad (6.8)$$

したがって, 集合  $\{\eta_i, |\phi_i\rangle\}_{i=1}^n$  の unambiguous discrimination は semidefinite programming (SDP) として定式化される. そして, この問題の課題は識別成功確率

$$p_o = \sum_{i=1}^n \eta_i x_i, \quad (6.9a)$$

を次のような条件の下で最大化することである.

$$x_i \geq 0 \quad (i = 1, 2, \dots, n), \quad (6.9b)$$

$$N - X \geq 0, \quad (6.9c)$$

ここで,  $X = \text{diag}(x_1, x_2, \dots, x_n)$  であり, 変数は  $x_i$  である. 解  $x_i$  は一意的に決まり, 最適な測定も一意的であることを示すことができる. 証明は後の 6.4 節で述べる.

### 6.1.2 Relaxed problem と状態の数の減少

Unambiguous discrimination の最適な戦略では、与えられた状態が状態  $|\phi_i\rangle$  のいくつかであると同定する確率が 0 であることがある。つまり、(6.9) 式で与えられた問題の解で  $x_i$  のいくつかは 0 であると推測される。この事象が起こった場合をうまく扱うためには、(6.9b) 式で与えられた  $x_i \geq 0$  という条件を緩和した問題を考えると便利である。この 2 つの問題を見分けるために、緩和された形式の問題を”relaxed  $n$ -state problem”と呼び、(6.9) 式で与えられた元の問題を単に” $n$ -state problem”と呼ぶ。

Relaxed  $n$ -state problem での課題は識別成功確率

$$p_o^R = \sum_{i=1}^n \eta_i x_i^R, \quad (6.10a)$$

を次のような条件の下で最大化することである。

$$N - X^R \geq 0, \quad (6.10b)$$

ここで、 $X^R = \text{diag}(x_1^R, x_2^R, \dots, x_n^R)$  である。また、relaxed problem での量を表すために上付き文字 R を用いた。

この 2 つの問題の解には重要な関係がある。 $x^R = (x_1^R, x_2^R, \dots, x_n^R)$  は relaxed  $n$ -state problem の解であるとする。そのとき、次のような性質があることを示すことができる。

- (I) もし、すべての  $i$  に対して、 $x_i^R \geq 0$  ならば、 $x^R$  は  $n$ -state problem の解である。
- (II) もし、空集合でないある指数の集合  $S$  のうちの  $i$  に対して、 $x_i^R < 0$  ならば、 $n$ -state problem の解は  $S$  の少なくとも 1 つの  $i$  に対して、 $x_i = 0$  である要素を持っている。

性質 (I) が成り立つことは明らかである。性質 (II) を示すために、次のような 2 つの解の線形補間を考える。

$$\hat{x}(\kappa) = (1 - \kappa) x + \kappa x^R, \quad 0 \leq \kappa \leq 1, \quad (6.11)$$

ここで、 $x$  は  $n$ -state problem の解であり、 $x^R$  は relaxed  $n$ -state problem の解である。 $\hat{x}(\kappa)$  は (6.9c) 式を満たすので、次のような関係が成り立つ。

$$N - \hat{X}(\kappa) = (1 - \kappa)(N - X) + \kappa(N - X^R) \geq 0. \quad (6.12)$$

また、 $\hat{x}(\kappa)$  に対応する識別成功確率は次のように与えられる。

$$\hat{p}(\kappa) = (1 - \kappa) p_{\max} + \kappa p_{\max}^R, \quad (6.13)$$

ここで、 $p_{\max}$  は  $n$ -state problem の最大識別成功確率であり、 $p_{\max}^R$  は relaxed  $n$ -state problem の最大識別成功確率である。ただし、定義により、 $p^R \geq p_{\max}$  であることに注意しなければならない。このことから、 $\hat{p}(\kappa)$  は  $0 \leq \kappa \leq 1$  に対して、 $p_{\max}$  よりも小さくはない。これは、もし、 $\hat{x}(\kappa)$  のすべての要素  $\hat{x}_i(\kappa)$  が非負であるならば、 $\hat{x}(\kappa)$  は  $n$ -state problem の解であることを意味する。

明らかに,  $\hat{x}_i(\kappa)$  は  $\kappa$  に関して連続である. また, すべての  $i$  に対して  $x_i \geq 0$  であること, そして,  $i \in S$  に対して  $x_i^R < 0$  である一方で, そうでなければ  $x_i^R \geq 0$  であることはわかっている. 図 6.1 で見られるように, 中間値の定理を用いると, すべての  $k$  に対して  $\hat{x}_k(\kappa_0) \geq 0$ , そして,  $i \in S$  に対して  $\hat{x}_i(\kappa_0) = 0$  であるような  $0 \leq \kappa_0 < 1$  が存在することに気づく. それゆえ,  $\hat{x}(\kappa_0)$  は  $n$ -state problem の解である. さらに,  $n$ -state problem の解は一意的であることから,  $\kappa_0 = 0$  であることが言える. したがって,  $n$ -state problem の解は集合  $S$  の少なくとも 1 つの  $i$  に対して  $x_i = 0$  である要素を持っているという結論を下すことができる.

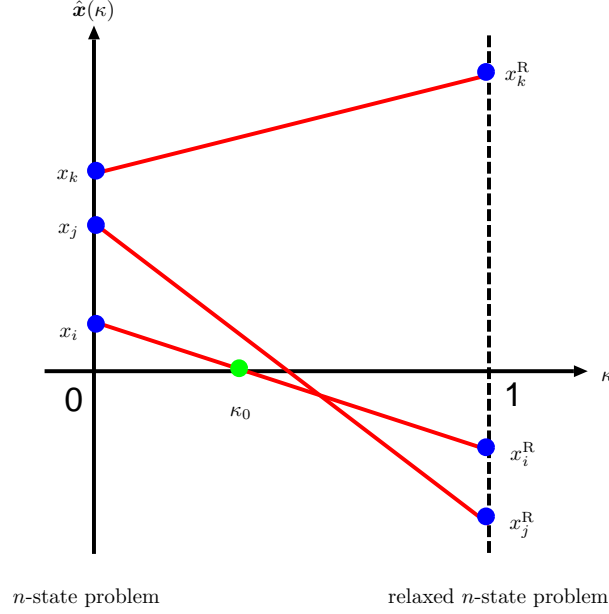


図 6.1:  $n$ -state problem の解と relaxed  $n$ -state problem の解の線形補間.

次に, もし, relaxed  $n$ -state problem の解でいくつかの  $x_i^R$  が負であるならば,  $n$ -state problem はある  $(n-1)$ -state problem に変換することができる. まず, 初めに, 1 つの要素だけが負である場合を仮定する. さらに, 一般性の損失なしに  $x_n^R < 0$  であり, その他は 0 でないと仮定することもできる. そのとき, 性質 (II) は  $n$ -state problem の解の要素  $x_n$  が 0 であることを示している. この解は元の  $n$ -state problem に対して  $x_n = 0$  という追加の条件を課すことで得ることができる. この追加の制限によって, (6.7) 式は

$$I_V - \sum_{i=1}^{n-1} x_i |\tilde{\phi}_i\rangle \langle \tilde{\phi}_i| \geq 0, \quad (6.14)$$

となる. また, 次のような 2 つの  $n-1$  個の状態の集合を定義する.

$$|\phi'_i\rangle \equiv \frac{Q|\phi_i\rangle}{\sqrt{\langle \phi_i|Q|\phi_i\rangle}} \quad (i = 1, 2, \dots, n-1), \quad (6.15)$$

$$|\tilde{\phi}'_i\rangle \equiv \sqrt{\langle \phi_i|Q|\phi_i\rangle} |\tilde{\phi}_i\rangle \quad (i = 1, 2, \dots, n-1), \quad (6.16)$$

ここで,  $Q$  は次のように定義される  $n-1$  個の状態  $\{|\tilde{\phi}_i\rangle\}_{i=1}^{n-1}$  によって張られた  $(n-1)$

次元部分空間  $V'$  上の射影演算子である.

$$Q \equiv I_V - |\phi_n\rangle\langle\phi_n|. \quad (6.17)$$

$\langle\tilde{\phi}'_i|\phi'_i\rangle = \delta_{ij}$  という意味で 2 つの状態の集合が相反であることは容易に証明することができる. さらに, (6.14) 式は次のように表すこともできる.

$$I_{V'} - \sum_{i=1}^{n-1} x'_i |\tilde{\phi}'_i\rangle\langle\tilde{\phi}'_i| \geq 0, \quad (6.18)$$

ここで,  $x'_i$  は次のように定義される.

$$x'_i \equiv \frac{x_i}{\langle\phi_i|Q|\phi_i\rangle}. \quad (6.19)$$

変換された  $(n-1)$ -state problem の  $x'_i$  が変数であることは簡単にわかる. したがって, 追加の制限  $x_n = 0$  を持つ  $n$ -state problem の識別成功確率は次のように書き直される.

$$\begin{aligned} p_o &= \sum_{i=1}^{n-1} \eta_i x_i \\ &= \left( \sum_{k=1}^{n-1} \eta_k \langle\phi_k|Q|\phi_k\rangle \right) \left( \sum_{i=1}^{n-1} \eta'_i x'_i \right), \end{aligned} \quad (6.20)$$

ここで,  $\eta'_i$  は次のように定義される.

$$\eta'_i \equiv \frac{\eta_i \langle\phi_i|Q|\phi_i\rangle}{\sum_{k=1}^{n-1} \eta_k \langle\phi_k|Q|\phi_k\rangle}. \quad (6.21)$$

ただし,  $\eta'_i > 0$  であり,  $\sum_{i=1}^{n-1} \eta'_i = 1$  であることに注意しなければならない. そして,  $\eta'_i$  は  $(n-1)$ -state problem での生起確率である. (6.18), (6.20) 式から, 追加の制限  $x_n = 0$  を持つ  $n$ -state problem は集合  $\{\eta'_i, |\phi'_i\rangle\}_{i=1}^{n-1}$  に対する  $(n-1)$ -state problem と等価であることに気づく. 以上から, 2 つの問題の最大識別成功確率と変数  $x_i$  は次のように関係付けられる.

$$p_{\max}^{(n)}[\{\eta_i, |\phi_i\rangle\}_{i=1}^n] = \left( \sum_{k=1}^{n-1} \eta_k \langle\phi_k|Q|\phi_k\rangle \right) p_{\max}^{(n-1)}[\{\eta'_i, |\phi'_i\rangle\}_{i=1}^{n-1}], \quad (6.22)$$

$$x_i = \langle\phi_i|Q|\phi_i\rangle x'_i. \quad (6.23)$$

しかしながら,  $x_n = 0$  という制限が状態  $|\phi_n\rangle$  を完全に無視するという意味ではないことを強調すべきである. これは (6.2) 式が  $|\phi_n\rangle$  を含むすべての状態に対して順守されなければならないからである. 変換された  $(n-1)$ -state problem での識別される状態は  $\{|\phi_i\rangle\}_{i=1}^{n-1}$  ではなく  $\{|\phi'_i\rangle\}_{i=1}^{n-1}$  である. そして, それはそれらの取り去られた  $|\phi_n\rangle$  要素を持つ正規化された状態である. (6.21) 式から見られるように, 生起確率も  $\langle\phi_i|Q|\phi_i\rangle$  の因子によって修正されている.

今のところ,  $x^R$  の 1 つの要素だけ負であることを仮定した. もし, 1 つより多くの要素が負であるならば, どの  $x_i$  ( $i \in S$ ) が  $n$ -state problem で無視されるかはわからな



い。それゆえ、集合  $S$  の  $i$  それぞれに対して、それに対応する 0 に固定された  $x_i$  を持つ  $(n-1)$ -state problem を解くことが必要とされる。そのとき、(6.22) 式から、 $n$ -state problem の最大識別成功確率の候補のいくつかを得るが、その中で最も大きい成功確率が  $n$ -state problem の解であることは明らかである。

また、 $x^R$  の負の要素の数が最大でも  $n-1$  個であることを示すことができる。これは次のような方法で見ることができる。状態  $\{|\phi_i\rangle\}_{i=1}^n$  が線形独立であることから、Gram 行列  $N$  は厳密に正定値である。これは十分に小さいが正である  $x_i^R$  の集合に対して条件式  $N - X^R \geq 0$  が満たされることを意味し、正の識別成功確率を導く。それゆえ、すべて負である要素を持つ  $x^R$  は relaxed  $n$ -state problem の解であるとはできない。

### 6.1.3 Relaxed problem の双対問題

まず、(6.10) 式で定義された relaxed  $n$ -state problem を解く。もし、すべての  $x_i^R$  が非負であるならば、それらは  $n$ -state problem の解を与える。前節で示したように、もし、 $x_i^R$  のいくつかが負であるならば、問題はある  $(n-1)$ -state problem に変換される。このようなとき、どのようにして relaxed  $n$ -state problem を解けばよいのだろうか。それには relaxed  $n$ -state problem の双対問題を考えると便利である。

双対問題での課題は次のように定義される

$$d \equiv \text{tr}[YN], \quad (6.24a)$$

を次のような条件の下で最小化することである。

$$Y \geq 0, \quad Y_{ii} = \eta_i, \quad (6.24b)$$

ここで、変数は  $n \times n$  Hermite 行列  $Y$  である。双対問題の最小値  $d_{\min}$  が (6.10) 式で定義された relaxed  $n$ -state problem の最大値  $p_{\max}^R$  に対して、上限を与えることは容易に示される。

$$\begin{aligned} p_{\max}^R &= \sum_{i=1}^n \eta_i x_i^R = \sum_{i=1}^n Y_{ii} x_i^R \\ &= \text{tr}[Y X^R] = \text{tr}[Y(N - (N - X^R))] \\ &\leq \text{tr}[YN] = d_{\min}, \end{aligned} \quad (6.25)$$

ここで、最後の行の不等式は  $\text{tr}[Y(N - X^R)] \geq 0$  という関係から得られる。それゆえ、次のように与えられる

$$(N - X^R)Y = 0, \quad (6.26)$$

と (6.10b), (6.24b) 式で与えられた条件は  $d_{\min}$  と  $p_{\max}^R$  が等しいための必要条件である。次節では、 $n=2$  と  $n=3$  の場合について、(6.24) 式で与えられる双対問題を解き、これらの条件を満たすことを明確に検証する。SDP の一般定理によると [37],  $n$ -state problem の解をこの方法で常に得られることが保証されている。

双対問題での変数である行列  $Y$  は (6.24b) 式によって、制約されている。任意の半正定値行列はあるベクトルの集合の Gram 行列で表すことができる。それゆえ、(6.24b) 式を満たすような  $Y$  は次のようにパラメータ化することができる。

$$Y_{ij} = \langle y_i | y_j \rangle, \quad (6.27)$$

ここで、 $|y_i\rangle$  はノルム  $\|y_i\| = \sqrt{\eta_i}$  を持つ任意のベクトルである。この便利なパラメータ化は次節でよく使われるので、覚えておく。

## 6.2 互いの内積が実数である場合

(6.10) 式で与えられた relaxed problem の解を得るために、(6.24) 式で与えられた双対問題を解く。もし、すべての  $x_i^R$  が非負であるならば、それらは (6.9) 式で与えられた緩和されていない元の主問題の解を与える。そうでなければ、問題は  $n - 1$  個の状態に対する問題に変換される。この計画がどのように解かれるのかを実証するために、まず、この計画によって 2 つの純粋状態の問題を解く。これは次に議論する 3 状態の問題に対して有益な指針をもたらす。

### 6.2.1 2 つの純粋状態の場合

双対問題の課題は

$$d = \text{tr}[YN], \quad (6.28)$$

を次のような条件の下で最小化することである。

$$Y \geq 0, \quad Y_{ii} = \eta_i, \quad (6.29)$$

ここで、 $Y$  は  $2 \times 2$  Hermite 行列である。状態  $|\phi_i\rangle$  の位相を変換することで、互いの内積が実数で負、つまり、 $\langle \phi_1 | \phi_2 \rangle = -|\langle \phi_1 | \phi_2 \rangle|$  であると仮定することができる。(6.27) 式で与えられたパラメータ化を用いて、 $d$  は次のように表すことができる。

$$d = 1 - (\langle y_1 | y_2 \rangle + \langle y_2 | y_1 \rangle) |\langle \phi_1 | \phi_2 \rangle|. \quad (6.30)$$

(6.30) 式の第 2 項に対して、三角不等式と Schwarz の不等式を適用すると、次のような不等式が得られる。

$$\begin{aligned} |\langle y_1 | y_2 \rangle + \langle y_2 | y_1 \rangle| &\leq 2|\langle y_1 | y_2 \rangle| \\ &\leq 2\sqrt{\langle y_1 | y_1 \rangle} \sqrt{\langle y_2 | y_2 \rangle} \\ &= 2\sqrt{\eta_1 \eta_2}, \end{aligned}$$

ここで、 $\langle \phi_i | \phi_i \rangle = \eta_i$  であることを用いた。この不等式によって、次のような  $d$  の最小値が与えられる。

$$d_{\min} = 1 - 2\sqrt{\eta_1 \eta_2} |\langle \phi_1 | \phi_2 \rangle|. \quad (6.31)$$

さらに、この最小値を達成するベクトル  $|y_i\rangle$  は次のような 1 次元ベクトルである。

$$|y_1\rangle = \sqrt{\eta_1}, \quad |y_2\rangle = \sqrt{\eta_2}.$$

したがって、 $Y$  は次のように与えられる。

$$Y = \begin{pmatrix} \eta_1 & \sqrt{\eta_1\eta_2} \\ \sqrt{\eta_2\eta_1} & \eta_2 \end{pmatrix} = \beta\beta^\dagger, \quad (6.32)$$

ここで、 $\beta$  は次のように定義される。

$$\beta \equiv \begin{pmatrix} \sqrt{\eta_1} \\ \sqrt{\eta_2} \end{pmatrix}.$$

実現可能条件は (6.26) 式によって与えられる。(6.26) 式の  $Y$  に代入し、 $\beta$  を右から掛けると、次のような方程式が得られる。

$$(N - X^R)\beta = 0, \quad (6.33)$$

ここで、 $\beta^\dagger\beta = 1$  であることを用いた。行列表示を用いることによって、(6.33) 式は次のように表すことができる。

$$\begin{pmatrix} 1 - x_1^R & -|\langle\phi_1|\phi_2\rangle| \\ -|\langle\phi_1|\phi_2\rangle| & 1 - x_2^R \end{pmatrix} \begin{pmatrix} \sqrt{\eta_1} \\ \sqrt{\eta_2} \end{pmatrix} = 0.$$

この方程式から、 $x_1^R, x_2^R$  は次のように与えられることが直ちにわかる。

$$\begin{aligned} x_1^R &= 1 - \sqrt{\frac{\eta_2}{\eta_1}} |\langle\phi_1|\phi_2\rangle|, \\ x_2^R &= 1 - \sqrt{\frac{\eta_1}{\eta_2}} |\langle\phi_1|\phi_2\rangle|. \end{aligned}$$

さらに、 $x_i^R$  は (6.10b) 式を満たさなければならない。つまり、 $N - X^R$  の固有値は非負でなければならない。 $N - X^R$  の固有値方程式は次のように与えられる。

$$\lambda \left( \lambda - \frac{|\langle\phi_1|\phi_2\rangle|}{\sqrt{\eta_1\eta_2}} \right) = 0.$$

そして、これは 2 つの固有値が非負であることを明らかに示す。それゆえ、 $x_i^R$  は 2 状態の relaxed problem の解である。

したがって、もし、 $x_i^R$  がすべて非負ならば、それらは次のような 2 状態の問題の最適解を与える。

$$x_1 = 1 - \sqrt{\frac{\eta_2}{\eta_1}} |\langle\phi_1|\phi_2\rangle|, \quad (6.34)$$

$$x_2 = 1 - \sqrt{\frac{\eta_1}{\eta_2}} |\langle\phi_1|\phi_2\rangle|. \quad (6.35)$$

そして、最大識別成功確率  $p_{\max}$  は  $d_{\min}$  によって、次のように与えられる。

$$p_{\max} = 1 - 2\sqrt{\eta_1\eta_2} |\langle \phi_1 | \phi_2 \rangle|. \quad (6.36)$$

しかしながら、もし、 $x_i^R$  の 1 つが負であるならば、識別される状態の 1 つを無視することが最適である。まず、 $x_2^R < 0$  であると仮定する。そして、それは生起確率と内積が次のような条件を満たすときに起こる。

$$\sqrt{\frac{\eta_2}{\eta_1}} < |\langle \phi_1 | \phi_2 \rangle|. \quad (6.37)$$

そのとき、 $x_2 = 0$  を持つ最適な解を探す必要がある。(6.15), (6.21) 式によると、追加の条件  $x_2 = 0$  を持つ 2 状態の問題は次のような生起確率  $\eta'_1$  を持つ  $|\phi'_1\rangle$  に対する 1 状態の問題と等価である。

$$|\phi'_1\rangle = \frac{Q|\phi_1\rangle}{\sqrt{\langle \phi_1 | Q | \phi_1 \rangle}}, \quad \eta'_1 = \frac{\eta_1 \langle \phi_1 | Q | \phi_1 \rangle}{\eta_1 \langle \phi_1 | Q | \phi_1 \rangle} = 1, \quad (6.38)$$

ここで、 $Q$  は  $Q = I - |\phi_2\rangle\langle\phi_2|$  で定義された射影演算子である。2 状態の問題の最大識別成功確率と変数  $x_i$ ,  $x'_i$  は次のように関係付けられる。

$$\begin{aligned} p_{\max}^{(2)}[\{\eta_i, |\phi_i\rangle\}_{i=1}^2] &= \eta_1 \langle \phi_1 | Q | \phi_1 \rangle p_{\max}^{(1)}[\{\eta'_1, |\phi'_1\rangle\}], \\ x_1 &= \langle \phi_1 | Q | \phi_1 \rangle x'_1, \end{aligned}$$

ここで、 $x'_1$  は 1 状態の問題の解である。

1 状態の問題は自明である。識別される状態は 1 つだけなので、 $p_{\max}^{(1)}[\{\eta'_1, |\phi'_1\rangle\}] = 1$ ,  $x'_1 = 1$  である。したがって、最大識別成功確率  $p_{\max}$  は次のように得られる。

$$p_{\max} = \eta_1 (1 - |\langle \phi_1 | \phi_2 \rangle|^2). \quad (6.39)$$

そして、 $x_i$  ( $i = 1, 2$ ) は次のように与えられる。

$$x_1 = 1 - |\langle \phi_1 | \phi_2 \rangle|^2, \quad (6.40a)$$

$$x_2 = 0. \quad (6.40b)$$

今、 $x_2^R < 0$  を仮定した。同様に、 $x_1^R < 0$  の場合に対しても、この問題は追加の条件  $x_1 = 0$  を持つ 2 状態の問題になることは明らかである。

以上から、最大識別成功確率  $p_{\max}$  と最適な解  $x_i$  は次のような方法でまとめられる。

$$(i) \quad \sqrt{\frac{\eta_2}{\eta_1}} < |\langle \phi_1 | \phi_2 \rangle| \text{ のとき}$$

$$p_{\max} = \eta_1 (1 - |\langle \phi_1 | \phi_2 \rangle|^2). \quad (6.41)$$

$$x_1 = 1 - |\langle \phi_1 | \phi_2 \rangle|^2, \quad (6.42a)$$

$$x_2 = 0. \quad (6.42b)$$

$$(ii) \quad |\langle \phi_1 | \phi_2 \rangle| \leq \sqrt{\frac{\eta_2}{\eta_1}} \leq \frac{1}{|\langle \phi_1 | \phi_2 \rangle|} \text{ のとき}$$

$$p_{\max} = 1 - 2\sqrt{\eta_1 \eta_2} |\langle \phi_1 | \phi_2 \rangle|. \quad (6.43)$$

$$x_1 = 1 - \sqrt{\frac{\eta_2}{\eta_1}} |\langle \phi_1 | \phi_2 \rangle|, \quad (6.44a)$$

$$x_2 = 1 - \sqrt{\frac{\eta_1}{\eta_2}} |\langle \phi_1 | \phi_2 \rangle|. \quad (6.44b)$$

$$(iii) \quad \frac{1}{|\langle \phi_1 | \phi_2 \rangle|} < \sqrt{\frac{\eta_2}{\eta_1}} \text{ のとき}$$

$$p_{\max} = \eta_2 (1 - |\langle \phi_1 | \phi_2 \rangle|^2). \quad (6.45)$$

$$x_1 = 0, \quad (6.46a)$$

$$x_2 = 1 - |\langle \phi_1 | \phi_2 \rangle|^2. \quad (6.46b)$$

これは2つの純粋状態の unambiguous discrimination のよく知られた結果を再現する。これらの結果は後の節で用いられるので、覚えておく。

### 6.2.2 3つの純粋状態の場合

生起確率  $\eta_i$  を持つ3つの純粋状態  $|\phi_i\rangle$  ( $i = 1, 2, 3$ ) の unambiguous discrimination を考察する。

状態の内積はそれらの状態の位相に依存する。しかしながら、次のように定義される  $\Gamma$  はそれぞれの状態のどんな位相変化に対しても不変である。

$$\Gamma \equiv \langle \phi_1 | \phi_2 \rangle \langle \phi_2 | \phi_3 \rangle \langle \phi_3 | \phi_1 \rangle. \quad (6.47)$$

それゆえ、少し考えれば、状態の位相変化によって、3つのお互いの内積の位相を同じに選べることがわかる。

ここで、 $\Gamma$  は実数であると仮定する。それは3つのお互いの内積の位相が実数であるように選ぶことを意味する。そこで、 $\Gamma \leq 0$  と  $\Gamma > 0$  の2つの場合を別々に考える。 $\Gamma$  が複素数の場合は次節で議論する。

#### A. $\Gamma \leq 0$ の場合

$\Gamma \leq 0$  の場合では、お互いの内積の位相は実数で負であるように選ぶことができる。これから見ていくように、2状態の問題と同様の方針で進められる。まず、 $d$  は次のように与えられる。

$$\begin{aligned} d = \text{tr}[YN] = 1 & - (\langle y_1 | y_2 \rangle + \langle y_2 | y_1 \rangle) |\langle \phi_1 | \phi_2 \rangle| \\ & - (\langle y_2 | y_3 \rangle + \langle y_3 | y_2 \rangle) |\langle \phi_2 | \phi_3 \rangle| \\ & - (\langle y_3 | y_1 \rangle + \langle y_1 | y_3 \rangle) |\langle \phi_3 | \phi_1 \rangle|. \end{aligned} \quad (6.48)$$

2 状態の問題と同様にして, 三角不等式と Schwarz の不等式を用いると, 直ちに, 次のような  $d$  の最小値が得られる.

$$d_{\min} = 1 - 2\sqrt{\eta_1\eta_2} |\langle \phi_1 | \phi_2 \rangle| - 2\sqrt{\eta_2\eta_3} |\langle \phi_2 | \phi_3 \rangle| - 2\sqrt{\eta_3\eta_1} |\langle \phi_3 | \phi_1 \rangle|. \quad (6.49)$$

そして, この下限を達成するベクトル  $|y_i\rangle$  は次のような 1 次元ベクトルである.

$$|y_1\rangle = \sqrt{\eta_1}, \quad |y_2\rangle = \sqrt{\eta_2}, \quad |y_3\rangle = \sqrt{\eta_3}.$$

したがって,  $Y$  は次のように表すことができる.

$$Y = \beta\beta^\dagger, \quad (6.50)$$

ここで,  $\beta$  は次のように定義される.

$$\beta = \begin{pmatrix} \sqrt{\eta_1} \\ \sqrt{\eta_2} \\ \sqrt{\eta_3} \end{pmatrix}.$$

(6.26) 式によって与えられた実現可能条件は  $\beta^\dagger\beta = 1$  であるから, 次のような形式をとる.

$$(N - X^R)\beta = 0. \quad (6.51)$$

行列表示を用いると, (6.51) 式は次のように表すことができる.

$$\begin{pmatrix} 1 - x_1^R & -|\langle \phi_1 | \phi_2 \rangle| & -|\langle \phi_3 | \phi_1 \rangle| \\ -|\langle \phi_1 | \phi_2 \rangle| & 1 - x_2^R & -|\langle \phi_2 | \phi_3 \rangle| \\ -|\langle \phi_3 | \phi_1 \rangle| & -|\langle \phi_2 | \phi_3 \rangle| & 1 - x_3^R \end{pmatrix} \begin{pmatrix} \sqrt{\eta_1} \\ \sqrt{\eta_2} \\ \sqrt{\eta_3} \end{pmatrix} = 0.$$

この方程式を解くことで, 次のような  $x_i^R$  ( $i = 1, 2, 3$ ) が得られる.

$$\begin{aligned} x_1^R &= 1 - \frac{1}{\sqrt{\eta_1}} (\sqrt{\eta_2} |\langle \phi_1 | \phi_2 \rangle| + \sqrt{\eta_3} |\langle \phi_3 | \phi_1 \rangle|), \\ x_2^R &= 1 - \frac{1}{\sqrt{\eta_2}} (\sqrt{\eta_1} |\langle \phi_1 | \phi_2 \rangle| + \sqrt{\eta_3} |\langle \phi_2 | \phi_3 \rangle|), \\ x_3^R &= 1 - \frac{1}{\sqrt{\eta_3}} (\sqrt{\eta_1} |\langle \phi_3 | \phi_1 \rangle| + \sqrt{\eta_2} |\langle \phi_2 | \phi_3 \rangle|). \end{aligned}$$

今,  $x_i^R$  が (6.10b) 式, つまり,  $N - X^R$  の半正定値性を満たすかを確認する. (6.51) 式で与えられた実現可能条件は  $N - X^R$  の固有値の 1 つが 0 であることを示す. 残り 2 つの固有値は次のような固有値方程式を解くことで決定される.

$$\lambda^2 - a\lambda + b = 0,$$

ここで, 係数  $a, b$  は次のように与えられる.

$$\begin{aligned} a &= \frac{\eta_1 + \eta_2}{\sqrt{\eta_1\eta_2}} |\langle \phi_1 | \phi_2 \rangle| + \frac{\eta_2 + \eta_3}{\sqrt{\eta_2\eta_3}} |\langle \phi_2 | \phi_3 \rangle| + \frac{\eta_3 + \eta_1}{\sqrt{\eta_3\eta_1}} |\langle \phi_3 | \phi_1 \rangle|, \\ b &= \frac{|\langle \phi_2 | \phi_3 \rangle \langle \phi_3 | \phi_1 \rangle|}{\sqrt{\eta_1\eta_2}} + \frac{|\langle \phi_3 | \phi_1 \rangle \langle \phi_1 | \phi_2 \rangle|}{\sqrt{\eta_2\eta_3}} + \frac{|\langle \phi_1 | \phi_2 \rangle \langle \phi_2 | \phi_3 \rangle|}{\sqrt{\eta_3\eta_1}}. \end{aligned}$$

実対称行列の固有値である 2 つの根は実数でなければならない。そして、 $a \geq 0, b \geq 0$  であるから、2 次方程式の解の公式はそれらが両方とも非負であることを示す。したがって、 $N - X^R$  の半正定値性は満たされる。それゆえ、 $x_i^R$  は relaxed problem の解である。

もし、すべての  $x_i^R$  が非負であるならば、 $x_i^R$  は元の 3 状態の問題の最適な解でもある。

$$x_1 = 1 - \frac{1}{\sqrt{\eta_1}} (\sqrt{\eta_2} |\langle \phi_1 | \phi_2 \rangle| + \sqrt{\eta_3} |\langle \phi_3 | \phi_1 \rangle|), \quad (6.52a)$$

$$x_2 = 1 - \frac{1}{\sqrt{\eta_2}} (\sqrt{\eta_1} |\langle \phi_1 | \phi_2 \rangle| + \sqrt{\eta_3} |\langle \phi_2 | \phi_3 \rangle|), \quad (6.52b)$$

$$x_3 = 1 - \frac{1}{\sqrt{\eta_3}} (\sqrt{\eta_1} |\langle \phi_3 | \phi_1 \rangle| + \sqrt{\eta_2} |\langle \phi_2 | \phi_3 \rangle|). \quad (6.52c)$$

そして、最大識別成功確率  $p_{\max}$  は  $d_{\min}$  によって次のように与えられる。

$$p_{\max} = 1 - 2\sqrt{\eta_1\eta_2} |\langle \phi_1 | \phi_2 \rangle| - 2\sqrt{\eta_2\eta_3} |\langle \phi_2 | \phi_3 \rangle| - 2\sqrt{\eta_3\eta_1} |\langle \phi_3 | \phi_1 \rangle|. \quad (6.53)$$

もし、いくつかの  $x_i^R$  が負であるならば、問題は 2 状態の問題に変換することができる。識別される 2 状態  $\{\eta'_i, |\phi'_i\rangle\}_{i=1}^2$  は (6.15), (6.21) 式の一般式によって決定される。元の問題の最大識別成功確率と解  $x_i$  は 2 状態の問題のよく知られた解に関して (6.22), (6.23) 式によって得ることができる。

## B. $\Gamma > 0$ の場合

$\Gamma > 0$  の場合では、お互いの内積の位相は実数で正であるように選ぶことができる。次のような 3 つの正の実数  $\alpha_i$  ( $i = 1, 2, 3$ ) を導入する。

$$\alpha_1 \equiv \sqrt{\frac{\langle \phi_1 | \phi_2 \rangle \langle \phi_3 | \phi_1 \rangle}{\langle \phi_2 | \phi_3 \rangle}}, \quad (6.54)$$

$$\alpha_2 \equiv \sqrt{\frac{\langle \phi_1 | \phi_2 \rangle \langle \phi_2 | \phi_3 \rangle}{\langle \phi_3 | \phi_1 \rangle}}, \quad (6.55)$$

$$\alpha_3 \equiv \sqrt{\frac{\langle \phi_2 | \phi_3 \rangle \langle \phi_3 | \phi_1 \rangle}{\langle \phi_1 | \phi_2 \rangle}}. \quad (6.56)$$

この  $\alpha_i$  を用いることで、内積は次のように表すことができる。

$$\langle \phi_1 | \phi_2 \rangle = \alpha_1 \alpha_2, \quad \langle \phi_2 | \phi_3 \rangle = \alpha_2 \alpha_3, \quad \langle \phi_3 | \phi_1 \rangle = \alpha_3 \alpha_1.$$

そのとき、 $d$  は次のように書き換えることができる。

$$\begin{aligned} d &= \sum_{i,j=1}^3 Y_{ij} N_{ji} \\ &= 1 + \sum_{i \neq j}^3 \alpha_i \alpha_j \langle y_i | y_j \rangle \\ &= 1 - \sum_{i=1}^3 \eta_i \alpha_i^2 + \left| \sum_{i=1}^3 \alpha_i | y_i \rangle \right|^2. \end{aligned} \quad (6.57)$$

今,  $d$  を最小化しなければならない. これは3つのベクトル  $\alpha_1|y_1\rangle, \alpha_2|y_2\rangle, \alpha_3|y_3\rangle$  の和のノルムである  $|\sum_{i=1}^3 \alpha_i|y_i\rangle|$  を最小化しなければならないことを意味する. ここで,  $|y_i\rangle$  はノルム  $\sqrt{\eta_i}$  を持つ任意のベクトルである.  $|\sum_{i=1}^3 \alpha_i|y_i\rangle|$  の最小値は3つの長さ  $\alpha_i\sqrt{\eta_i}$  が次のような関係を満たすかどうかによって決定される.

$$\alpha_1\sqrt{\eta_1} \leq \alpha_2\sqrt{\eta_2} + \alpha_3\sqrt{\eta_3}, \quad (6.58a)$$

$$\alpha_2\sqrt{\eta_2} \leq \alpha_1\sqrt{\eta_1} + \alpha_3\sqrt{\eta_3}, \quad (6.58b)$$

$$\alpha_3\sqrt{\eta_3} \leq \alpha_1\sqrt{\eta_1} + \alpha_2\sqrt{\eta_2}. \quad (6.58c)$$

これらの関係は3つのベクトル  $\alpha_i|y_i\rangle$  が三角形を形成するための条件である. そして, これ以降, それを三角条件と呼ぶことにする.

まず, (6.58) 式で与えられる三角条件を満たすと仮定する.  $|\sum_{i=1}^3 \alpha_i|y_i\rangle|$  の最小値は0である. そして, その最小値は  $\alpha_1y_1 + \alpha_2y_2 + \alpha_3y_3 = 0$  であるような  $|y_i| = \sqrt{\eta_i}$  を持つ1次元複素ベクトル  $|y_i\rangle = y_i$  によって達成される. そのとき,  $d$  の最小値は次のように与えられる.

$$d_{\min} = 1 - \sum_{i=1}^3 \eta_i \alpha_i^2. \quad (6.59)$$

また,  $Y$  は  $Y = \mathbf{y}^* \mathbf{y}^T$  で与えられる. ここで,  $\mathbf{y}$  は次のように定義される.

$$\mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix},$$

したがって, (6.26) 式は次のように書き換えられる.

$$(N - X^R) \mathbf{y}^* = 0.$$

そして, この式から,  $x_1^R, x_2^R, x_3^R$  に対する次のような3つの方程式が得られる.

$$(1 - x_1^R) y_1^* + \alpha_1 \alpha_2 y_2^* + \alpha_1 \alpha_3 y_3^* = 0, \quad (6.60)$$

$$\alpha_2 \alpha_1 y_1^* + (1 - x_2^R) y_2^* + \alpha_2 \alpha_3 y_3^* = 0, \quad (6.61)$$

$$\alpha_3 \alpha_1 y_1^* + \alpha_3 \alpha_2 y_2^* + (1 - x_3^R) y_3^* = 0. \quad (6.62)$$

今,  $\alpha_1 y_1 + \alpha_2 y_2 + \alpha_3 y_3 = 0$  という関係が成り立つことから, 最初の方程式は次のように書き換えられる.

$$(1 - x_1^R - \alpha_1^2) y_1^* = 0.$$

$y_1^* \neq 0$  であることから,  $x_1^R = 1 - \alpha_1^2$  が得られる. 同様にして, 次のような  $x_2^R, x_3^R$  が得られる.

$$x_1^R = 1 - \alpha_1^2,$$

$$x_2^R = 1 - \alpha_2^2,$$

$$x_3^R = 1 - \alpha_3^2.$$



$N - X^R$  の半正定値性は簡単に見ることができる。なぜならば、 $N - X^R$  は次のように表すことができるからである。

$$N - X^R = \alpha \alpha^\dagger,$$

ここで、 $\alpha$  は次のように定義される。

$$\alpha = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}.$$

したがって、得られた  $x_i^R$  は 3 状態の relaxed problem の最適な解である。

もし、すべての  $x_i^R$  が非負であるならば、それらは元の 3 状態の問題の最適な解  $x_i$  である。

$$x_1 = 1 - \alpha_1^2, \quad (6.63a)$$

$$x_2 = 1 - \alpha_2^2, \quad (6.63b)$$

$$x_3 = 1 - \alpha_3^2. \quad (6.63c)$$

そして、最大識別成功確率  $p_{\max}$  は  $d_{\min}$  によって、次のように与えられる。

$$p_{\max} = 1 - (\eta_1 \alpha_1^2 + \eta_2 \alpha_2^2 + \eta_3 \alpha_3^2). \quad (6.64)$$

もし、 $x_i^R$  のいくつかが負であるならば、前に記述したように、2 状態の問題に変換することで問題は解くことができる。

次に、(6.58) 式で与えられる三角条件を満たさない場合を考える。 $|\sum_{i=1}^3 \alpha_i |y_i\rangle|$  は  $\alpha_1|y_1\rangle, \alpha_2|y_2\rangle, \alpha_3|y_3\rangle$  のノルムを比較して、3 つのノルムのうち、1 番大きいものから残り 2 つのノルムを引くことで最小化されることがわかる。 $\alpha_1\sqrt{\eta_1} \geq \alpha_2\sqrt{\eta_2}, \alpha_3\sqrt{\eta_3}$  であるとする。そのとき、 $d$  の最小値は次のように与えられる。

$$\begin{aligned} d_{\min} &= 1 - \sum_{i=1}^3 \eta_i \alpha_i^2 + (\alpha_1\sqrt{\eta_1} - \alpha_2\sqrt{\eta_2} - \alpha_3\sqrt{\eta_3})^2 \\ &= 1 - 2\sqrt{\eta_1\eta_2}\alpha_1\alpha_2 + 2\sqrt{\eta_2\eta_3}\alpha_2\alpha_3 - 2\sqrt{\eta_3\eta_1}\alpha_3\alpha_1. \end{aligned} \quad (6.65)$$

そして、この最小値を達成するベクトル  $|y_i\rangle$  は次のような 1 次元ベクトルである。

$$|y_1\rangle = -\sqrt{\eta_1}, \quad |y_2\rangle = -\sqrt{\eta_2}, \quad |y_3\rangle = -\sqrt{\eta_3}.$$

したがって、 $Y$  は次のように与えられる。

$$Y = \beta \beta^\dagger,$$

ここで、 $\beta$  は次のように定義される。

$$\beta = \begin{pmatrix} \sqrt{\eta_1} \\ -\sqrt{\eta_2} \\ -\sqrt{\eta_3} \end{pmatrix}.$$

後の議論は  $\Gamma \leq 0$  の場合と全く同様の方法で進められる.  $Y = \beta\beta^\dagger$  であるから, (6.26) 式で与えられる実現可能条件は次のように書き換えられる.

$$(N - X^R) \beta = 0. \quad (6.66)$$

そして, その行列表現は次のように与えられる.

$$\begin{pmatrix} 1 - x_1^R & \alpha_1\alpha_2 & \alpha_1\alpha_3 \\ \alpha_2\alpha_1 & 1 - x_2^R & \alpha_2\alpha_3 \\ \alpha_3\alpha_1 & \alpha_3\alpha_2 & 1 - x_3^R \end{pmatrix} \begin{pmatrix} \sqrt{\eta_1} \\ -\sqrt{\eta_2} \\ -\sqrt{\eta_3} \end{pmatrix} = 0.$$

この方程式を解くことで, 次のような  $x_i^R$  が得られる.

$$\begin{aligned} x_1^R &= 1 - \frac{\alpha_1}{\sqrt{\eta_1}} (\alpha_2\sqrt{\eta_2} + \alpha_3\sqrt{\eta_3}), \\ x_2^R &= 1 - \frac{\alpha_2}{\sqrt{\eta_2}} (\alpha_1\sqrt{\eta_1} - \alpha_3\sqrt{\eta_3}), \\ x_3^R &= 1 - \frac{\alpha_3}{\sqrt{\eta_3}} (\alpha_1\sqrt{\eta_1} - \alpha_2\sqrt{\eta_2}). \end{aligned}$$

$N - X^R$  の半正定値性は次のような方法で証明される.  $N - X^R$  の固有値の 1 つは 0 である. そして, それは (6.66) 式から見る事ができる. 残りの 2 つの固有値は次のような 2 次方程式の根によって与えられる.

$$\lambda^2 - a\lambda + b = 0,$$

ここで, 係数  $a, b$  は次のように与えられる.

$$\begin{aligned} a &= \frac{\alpha_1}{\sqrt{\eta_1}} (\alpha_2\sqrt{\eta_2} + \alpha_3\sqrt{\eta_3}) + \frac{\alpha_2}{\sqrt{\eta_2}} (\alpha_1\sqrt{\eta_1} - \alpha_3\sqrt{\eta_3}) + \frac{\alpha_3}{\sqrt{\eta_3}} (\alpha_1\sqrt{\eta_1} - \alpha_2\sqrt{\eta_2}), \\ b &= \frac{\alpha_1\alpha_2\alpha_3}{\sqrt{\eta_1\eta_2\eta_3}} (\alpha_1\sqrt{\eta_1} - \alpha_2\sqrt{\eta_2} - \alpha_3\sqrt{\eta_3}). \end{aligned}$$

今,  $\alpha_1\sqrt{\eta_1} \geq \alpha_2\sqrt{\eta_2}, \alpha_3\sqrt{\eta_3}$  であることを仮定している. そして, それは (6.58a) 式を破ることを意味する. したがって,  $a \geq 0, b \geq 0$  であることがわかる. それゆえ, 残りの 2 つの固有値も非負である. したがって,  $x_i^R$  は 3 状態の relaxed problem の解である.

もし, すべての  $x_i^R$  が正であるならば,  $x_i^R$  は元の 3 状態の問題の最適な解  $x_i$  である.

$$x_1 = 1 - \frac{1}{\sqrt{\eta_1}} (\sqrt{\eta_2} |\langle \phi_1 | \phi_2 \rangle| + \sqrt{\eta_3} |\langle \phi_3 | \phi_1 \rangle|), \quad (6.67a)$$

$$x_2 = 1 - \frac{1}{\sqrt{\eta_2}} (\sqrt{\eta_1} |\langle \phi_1 | \phi_2 \rangle| - \sqrt{\eta_3} |\langle \phi_2 | \phi_3 \rangle|), \quad (6.67b)$$

$$x_3 = 1 - \frac{1}{\sqrt{\eta_3}} (\sqrt{\eta_1} |\langle \phi_3 | \phi_1 \rangle| - \sqrt{\eta_2} |\langle \phi_2 | \phi_3 \rangle|). \quad (6.67c)$$

そして, 最大識別成功確率  $p_{\max}$  は  $d_{\min}$  によって次のように与えられる.

$$p_{\max} = 1 - 2\sqrt{\eta_1\eta_2} |\langle \phi_1 | \phi_2 \rangle| + 2\sqrt{\eta_2\eta_3} |\langle \phi_2 | \phi_3 \rangle| - 2\sqrt{\eta_3\eta_1} |\langle \phi_3 | \phi_1 \rangle|. \quad (6.68)$$

上の結果での項の符号の明らかな非対称性は  $\alpha_1\sqrt{\eta_1} \geq \alpha_2\sqrt{\eta_2}, \alpha_3\sqrt{\eta_3}$  という仮定に起因していることに注意しなければならない.

もし,  $x_i^R$  のいくつかが負であるならば, 他の場合と同じように, 適切な 2 状態の問題を考えることで解析解を常に得ることができる.

### 6.2.3 例

次のような3つのベクトルの集合を考える.

$$|\phi_1\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad |\phi_2\rangle = \begin{pmatrix} \cos \varphi_2 \\ \sin \varphi_2 \\ 0 \end{pmatrix}, \quad |\phi_3\rangle = \begin{pmatrix} \cos \varphi_3 \sin \theta_3 \\ \sin \varphi_3 \sin \theta_3 \\ \cos \theta_3 \end{pmatrix}.$$

まず, 1つめの例として, 図 6.2 では, それぞれの生起確率が等しいと仮定し, それぞれ  $\varphi_2 = \pi/3$ ,  $\varphi_3 = \pi/4$  に固定した場合の最適な解  $x_i$  と最大識別成功確率  $p_{\max}$  を  $\theta_3$  の関数として表示している.  $\theta_3$  を 0 から  $\pi/2$  まで変化させていくと, 最適な解のタイプが変わっていく.  $\theta_3$  が小さいとき, 3つの状態のすべては有限の識別確率  $x_i$  を持っている.  $\theta_3$  が大きくなるにつれて, 0 になることがない  $x_i$  を持つ状態の数は減っていく. これは状態  $|\phi_3\rangle$  が状態  $|\phi_2\rangle$  に近づくことでそれら2つの状態を識別することが難しくなるという事実を反映している. また,  $\theta_3$  が 0.18(rad) から 1.01(rad) までの範囲にあるとき,  $x_1, x_2$  は一定である. それは  $\Gamma > 0$  の場合に3つの長さ  $\alpha_i \sqrt{\eta_i}$  が (6.58) 式で与えられる三角条件を満たすときである. そのような場合,  $x_i$  は (6.63) 式で与えられるように, お互いの内積だけで表すことができる.

$$\begin{aligned} x_1 &= 1 - \frac{\cos \varphi_2 \cos \varphi_3}{\cos(\varphi_2 - \varphi_3)}, \\ x_2 &= 1 - \frac{\cos \varphi_2 \cos(\varphi_2 - \varphi_3)}{\cos \varphi_3}, \\ x_3 &= 1 - \frac{\cos \varphi_3 \cos(\varphi_2 - \varphi_3)}{\cos \varphi_2} \sin^2 \theta_3. \end{aligned}$$

$x_1, x_2$  が  $\theta_3$  に依らないことは明らかである. したがって,  $x_1, x_2$  はこの範囲では一定である.

2つめの例として, 図 6.3 では, 3つの状態を  $\varphi_2 = \pi/3$ ,  $\varphi_3 = \pi/4$ ,  $\theta_3 = \pi/5$  に固定して, それぞれの生起確率は  $\eta_1 = \eta_2$  を仮定し,  $\eta_3$  を 0 から 1 まで変化させたときの最適な解  $x_i$  と最大識別成功確率  $p_{\max}$  を  $\eta_3$  の関数として表示している. 十分に小さい  $\eta_3$  に対して, 最適な解は  $x_3 = 0$  を与える. 予期されたように,  $\eta_3$  が 1 に近づくにつれて, 状態  $|\phi_3\rangle$  だけが生き残る. しかしながら, 最大識別成功確率は 1 に近づかない. これは  $\eta_i \neq 0$  を仮定し,  $\eta_i$  のいくつかがとても小さいとしても, すべての状態に対して (6.2) 式で与えられる識別に間違いが許されないという条件が課されているからである. また, 興味深いことが1つある. それは  $\Gamma > 0$  で (6.58) 式で与えられる三角条件を満たす場合である. (6.63) 式は  $x_i$  が  $\eta_i$  に依らないことを示している. つまり, 最適な測定は生起確率に依らないことを示している. これが  $\eta_3$  が 0.05 から 0.7 の範囲にあるときにすべての  $x_i$  が一定である理由である.

この節を終える前に, unambiguous discrimination は semidefinite programming(SDP) として定式化することができるので, 数値的に解くことができることに言及する. 上の例について, SDPA [40] というパッケージを用いて, 数値解析を行った. そして, 念のために, 2つの結果を比較した. それによって, 数値解析の解は数値誤差の範囲内で解析的な解を再現することが証明された.

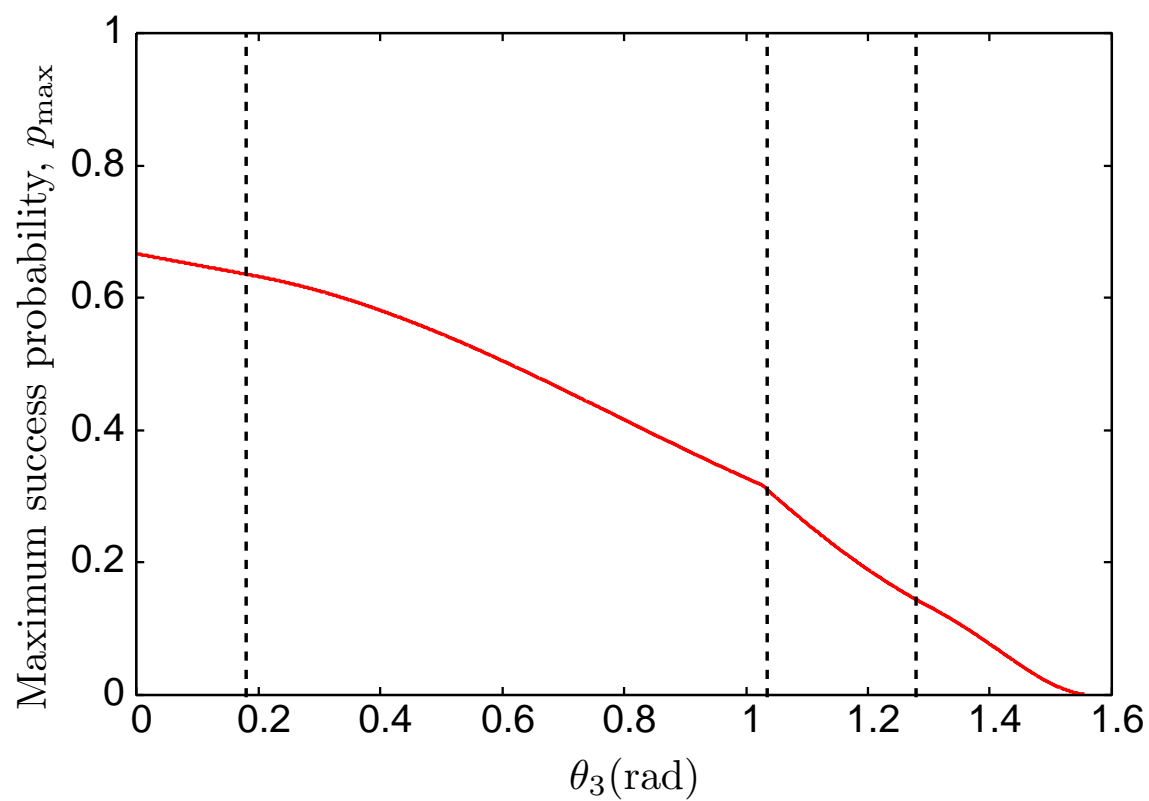
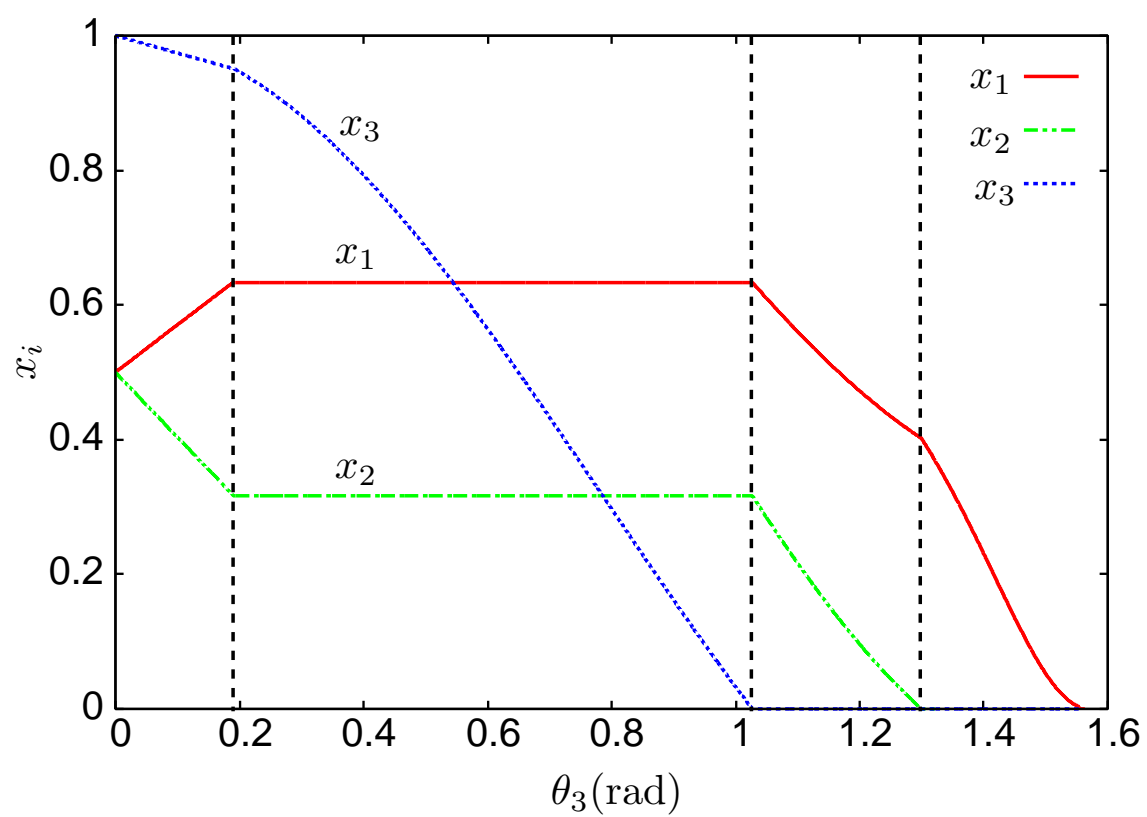


図 6.2:  $\theta_3$  に対する  $x_i$ (上部) と最大識別成功確率 (下部).

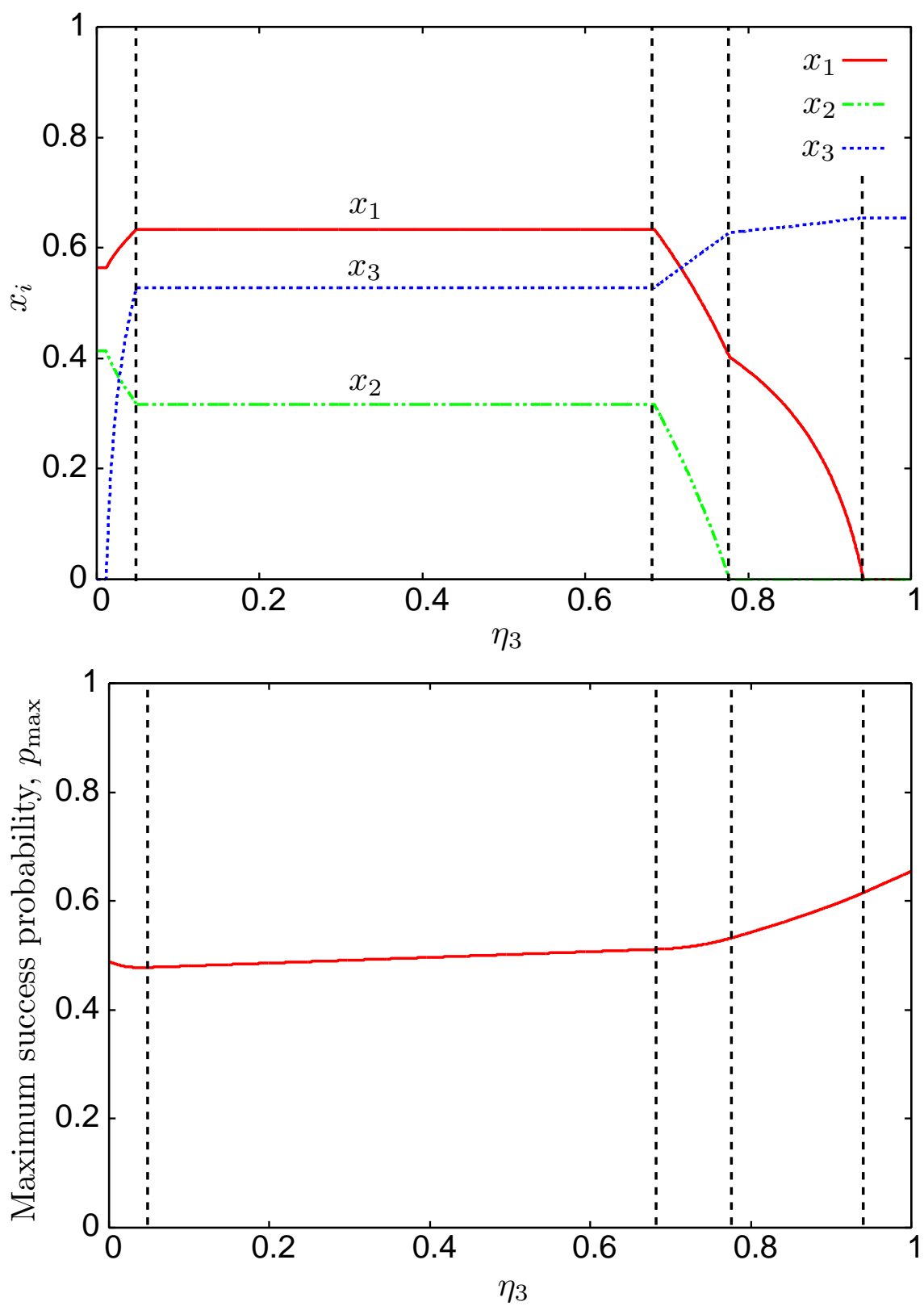


図 6.3:  $\eta_3$  に対する  $x_i$ (上部) と最大識別成功確率 (下部).

### 6.3 互いの内積が複素数である場合

前節では、お互いの内積が実数であり、一般の生起確率を持つ3つの純粋状態の unambiguous discrimination に対して完全に解析的な解が得られた。ここでは、お互いの内積が複素数の場合について分析するが、我々の方法は一般の複素数の場合には応用できない。しかしながら、ある特別な場合に解析解が得られたので、その例を示す。

前節と同じように、次のような  $\Gamma$  を定義する。

$$\Gamma = \langle \phi_1 | \phi_2 \rangle \langle \phi_2 | \phi_3 \rangle \langle \phi_3 | \phi_1 \rangle = |\Gamma| e^{3i\theta}, \quad (6.69)$$

ここで、 $0 \leq \theta < 2\pi/3$  である。3つの状態の位相を選ぶことができるので、内積  $\langle \phi_1 | \phi_2 \rangle$ ,  $\langle \phi_2 | \phi_3 \rangle$ ,  $\langle \phi_3 | \phi_1 \rangle$  の位相は同じ値  $\theta$  にとることができる。そのとき、3つの内積は次のような方法で表すことができる。

$$\langle \phi_1 | \phi_2 \rangle = \alpha_1 \alpha_2 e^{i\theta}, \quad (6.70)$$

$$\langle \phi_2 | \phi_3 \rangle = \alpha_2 \alpha_3 e^{i\theta}, \quad (6.71)$$

$$\langle \phi_3 | \phi_1 \rangle = \alpha_3 \alpha_1 e^{i\theta}, \quad (6.72)$$

ここで、正の実数  $\alpha_i$  は次のように内積の絶対値で定義される。

$$\alpha_1 \equiv \sqrt{\frac{|\langle \phi_1 | \phi_2 \rangle| |\langle \phi_3 | \phi_1 \rangle|}{|\langle \phi_2 | \phi_3 \rangle|}}, \quad (6.73)$$

$$\alpha_2 \equiv \sqrt{\frac{|\langle \phi_1 | \phi_2 \rangle| |\langle \phi_2 | \phi_3 \rangle|}{|\langle \phi_3 | \phi_1 \rangle|}}, \quad (6.74)$$

$$\alpha_3 \equiv \sqrt{\frac{|\langle \phi_2 | \phi_3 \rangle| |\langle \phi_3 | \phi_1 \rangle|}{|\langle \phi_1 | \phi_2 \rangle|}}. \quad (6.75)$$

$Y$  はノルム  $\sqrt{\eta_i}$  を持つ任意のベクトル  $|y_i\rangle$  の Gram 行列  $Y_{ij} = \langle y_i | y_j \rangle$  で与えられるので、 $d$  は次のように表すことができる。

$$d = 1 + \langle \langle A | D | A \rangle \rangle, \quad (6.76)$$

ここで、 $|A\rangle\rangle$  は次のような3要素ベクトルで定義される。

$$|A\rangle\rangle = \begin{pmatrix} \alpha_1 |y_1\rangle \\ \alpha_2 |y_2\rangle \\ \alpha_3 |y_3\rangle \end{pmatrix}, \quad (6.77)$$

また、 $D$  は次のような  $3 \times 3$  行列で与えられる。

$$D = \begin{pmatrix} 0 & e^{-i\theta} & e^{i\theta} \\ e^{i\theta} & 0 & e^{-i\theta} \\ e^{-i\theta} & e^{i\theta} & 0 \end{pmatrix}. \quad (6.78)$$

行列  $D$  は Hermite 行列であることから, 容易に対角化することができる.

$$U^\dagger D U = \text{diag}(\lambda_1, \lambda_2, \lambda_3), \quad (6.79)$$

ここで,  $U$  は次のような 1 の 3 乗根  $\omega \equiv e^{i\frac{2}{3}\pi}$  を用いた Unitary 行列で定義される.

$$U = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}. \quad (6.80)$$

さらに,  $D$  の固有値は次のように与えられる.

$$\lambda_1 = 2 \cos \theta, \quad \lambda_2 = 2 \cos \left( \theta - \frac{2}{3}\pi \right), \quad \lambda_3 = 2 \cos \left( \theta + \frac{2}{3}\pi \right). \quad (6.81)$$

今, (6.76) 式で与えられた  $d$  は次のような方法で表すことができる.

$$d = 1 + \frac{1}{3} (\lambda_1 \|a_1\|^2 + \lambda_2 \|a_2\|^2 + \lambda_3 \|a_3\|^2), \quad (6.82)$$

ここで, 3 つのベクトル  $|a_i\rangle$  は次のように定義される.

$$\begin{pmatrix} |a_1\rangle \\ |a_2\rangle \\ |a_3\rangle \end{pmatrix} = \sqrt{3} U^\dagger |A\rangle = \begin{pmatrix} \alpha_1 |y_1\rangle + \alpha_2 |y_2\rangle + \alpha_3 |y_3\rangle \\ \alpha_1 |y_1\rangle + \omega^2 \alpha_2 |y_2\rangle + \omega \alpha_3 |y_3\rangle \\ \alpha_1 |y_1\rangle + \omega \alpha_2 |y_2\rangle + \omega^2 \alpha_3 |y_3\rangle \end{pmatrix}, \quad (6.83)$$

(6.82) 式で与えられた式は  $d$  が 3 つのベクトル  $|a_i\rangle$  のノルムの 2 乗の線形結合であることを示す. 今,  $|y_i\rangle$  は自身のノルムが  $\|y_i\| = \sqrt{\eta_i}$  であるという 1 つだけの制限を持った任意のベクトルである. したがって,  $|a_i\rangle$  それぞれのノルムの最大値および最小値は簡単に得られる. もし, 3 つの長さ  $\alpha_i \sqrt{\eta_i}$  が (6.58) 式で与えられた三角条件を満たすならば,  $\|a_i\|$  の最小値は 0 である. 一方, 三角条件を満たさない場合, 最小値は  $\alpha_1 \sqrt{\eta_1} - \alpha_2 \sqrt{\eta_2} - \alpha_3 \sqrt{\eta_3}$  で与えられる. ただし, ここでは,  $\alpha_1 \sqrt{\eta_1}$  がすべての  $\alpha_i \sqrt{\eta_i}$  のうちで 1 番大きいことを仮定した. また,  $\|a_i\|$  の最大値は  $\alpha_1 \sqrt{\eta_1} + \alpha_2 \sqrt{\eta_2} + \alpha_3 \sqrt{\eta_3}$  で与えられることは明らかである. さらに,  $|a_i\rangle$  の 3 つのノルムの 2 乗の和は定数であることもわかる.

$$\sum_{i=1}^3 \|a_i\|^2 = 3 \langle A | A \rangle = 3 \sum_{i=1}^3 \alpha_i^2 \eta_i. \quad (6.84)$$

この恒等式を用いて,  $d$  は  $|a_i\rangle$  のノルムの 2 乗の任意のペアで書き換えることができる. それでも, それを解析的に最小化することは難しい. しかしながら, もし, 固有値  $\lambda_i$  の 2 つが等しければ,  $d$  は 1 つのベクトル  $|a_i\rangle$  のノルムの 2 乗で表すことができ, とても簡単に最小化することができる. そして, これは  $\theta = 0$  と  $\theta = \pi/3$  のときにだけ起こることがわかる. それら 2 つの場合は  $\Gamma$  が実数の場合に対応することは明らかである. そして, それは前節で解かれている. また, このような場合, 前と同じ結果を得られることが証明される.

たとえ  $\Gamma$  が複素数であっても、解析的な解を簡単に得られる例が 1 つある。これは 3 つの長さ  $\alpha_i \sqrt{\eta_i}$  がお互いに等しい場合である。(6.84) 式を用いて、 $||a_3\rangle|$  を消去すると、 $d$  は次のように書き換えられる。

$$d = 1 + \lambda_3 \sum_{i=1}^3 \alpha_i^2 \eta_i + \frac{1}{3} [(\lambda_1 - \lambda_3) ||a_1\rangle|^2 + (\lambda_2 - \lambda_3) ||a_2\rangle|^2]. \quad (6.85)$$

もし、 $\alpha_i \sqrt{\eta_i}$  が一定であるならば、2 つのノルム  $||a_1\rangle|$ ,  $||a_2\rangle|$  は同時に 0 にできることがわかる。これは、例えば、次のような 3 つのベクトル  $\alpha_i |y_i\rangle$  が複素平面上で正三角形を成す単一成分の複素ベクトルであるように  $|y_i\rangle$  を選ぶことで可能である。

$$|y_1\rangle = \sqrt{\eta_1}, \quad |y_2\rangle = \sqrt{\eta_2} \omega, \quad |y_3\rangle = \sqrt{\eta_3} \omega. \quad (6.86)$$

ただし、 $\lambda_1 \geq \lambda_3$ ,  $\lambda_2 \geq \lambda_3$  であることに注意しなければならない。したがって、 $d$  の最小値は次のように与えられる。

$$d_{\min} = 1 + 2 \cos \left( \theta + \frac{2}{3} \pi \right) \sum_{i=1}^3 \alpha_i^2 \eta_i. \quad (6.87)$$

(6.26) 式で与えられる実現可能条件は  $x_i^R$  が次のような形式で与えられることを要請する。

$$x_i^R = 1 + 2\alpha_i^2 \cos \left( \theta + \frac{2}{3} \pi \right). \quad (6.88)$$

さらに、 $N - X^R$  の半正定値性は次のような方法で証明される。

$$N - X^R = \text{diag}(\alpha_1, \alpha_2, \alpha_3) (D^* - \lambda_3 I) \text{diag}(\alpha_1, \alpha_2, \alpha_3) \geq 0, \quad (6.89)$$

ここで、 $D^*$  は (6.78) 式で与えられた行列  $D$  の複素共役である。そして、 $\lambda_3$  は  $D^*$  の最も小さい固有値でもあるので、このような不等式が成り立つ。それゆえ、(6.88) 式で与えられた  $x_i^R$  は relaxed problem の解である。もし、すべての  $x_i^R$  が非負であるならば、それらは元の 3 状態の問題の解でもある。そのとき、最大識別成功確率  $p_{\max}$  は  $d_{\min}$  によって次のように与えられる。

$$p_{\max} = d_{\min} = 1 + 2 \cos \left( \theta + \frac{2}{3} \pi \right) \sum_{i=1}^3 \alpha_i^2 \eta_i. \quad (6.90)$$

そうでなければ、問題はある 2 状態の問題に変換される。

この結果は、状態の数が 3 つの場合に限られるが、参考文献 [24] で考えられた対称な状態の一般化である。対称な状態に関して、お互いの内積の絶対値のすべては同じ ( $\alpha_i$  が一定である) であり、生起確率  $\eta_i$  は等しいと仮定される。この場合では、 $x_i^R$  は非負で同一であることが示される。そして、最大識別成功確率は次のように与えられる。

$$p_{\max} = 1 + 2\gamma \cos \left( \theta + \frac{2}{3} \pi \right), \quad (6.91)$$

ここで、 $\gamma = ||\langle \phi_1 | \phi_2 \rangle|| = ||\langle \phi_2 | \phi_3 \rangle|| = ||\langle \phi_3 | \phi_1 \rangle||$  である。



## 6.4 解の一意性

第6章を終える前に,  $n$ -state problem の解の一意性について述べる. まず, 次のような2つの命題が成り立つ.

命題1. もし,  $x, x'$  の両方が  $n$ -state problem の解であるならば, 少なくとも1つの  $i_0$  に対して,  $x_{i_0} = x'_{i_0}$  である.

命題2. 要素の1つ  $x_{i_0}$  がある値に固定されているという追加の条件を持つ  $n$ -state problem を考える. 解が存在すると仮定すると, 残りの変数はゼロかある  $r$ -state problem によって一意的に決まる. ここで,  $1 \leq r \leq n-1$  である.

これら2つの命題と一緒に,  $n$ -state problem の解の一意性は状態の数  $n$  についての数学的帰納法によって, 結果として生じる. まず,  $n=1$  のときは明白である. 次に,  $r \leq n-1$  に対する  $r$ -state problem では解は一意であると仮定する. さらに,  $x, x'$  は  $n$ -state problem の解であるとする. 命題1によって, ある  $i_0$  に対して  $x_{i_0} = x'_{i_0}$  を持つ. 命題2は残りの変数がある  $r$ -state problem によって決定されることを述べている. ここで,  $1 \leq r \leq n-1$  である. その仮定によって,  $x = x'$  であると結論を下せる.

今, 2つの命題の証明を述べる.

命題1. の証明 もし,  $N-X > 0$  ならば, 識別成功確率を増加させると同時に,  $N-X \geq 0$  を満たすように任意の要素  $x_i$  に十分小さな  $\epsilon (> 0)$  を加えることができる. それゆえ, もし,  $x$  が解であるならば,  $\det(N-X) = 0$  である. 2つの解の凸の線形結合も解であることから, 次のような関係が得られる.

$$\det[N - \kappa X - (1 - \kappa) X'] = 0 \quad (0 \leq \kappa \leq 1). \quad (6.92)$$

この行列式の  $\kappa^n$  の項の係数は次のように与えられる.

$$(x'_1 - x_1)(x'_2 - x_2) \cdots (x'_n - x_n). \quad (6.93)$$

そして, それはゼロでなければならない. これはある  $i_0$  に対して  $x_{i_0} = x'_{i_0}$  であることを意味する. ■

命題2. の証明 一般性の損失なしに,  $i_0 = n$  を仮定する. (6.7) 式で与えられる条件は次のように表すことができる.

$$\Delta - \sum_{i=1}^{n-1} x_i |\tilde{\phi}_i\rangle \langle \tilde{\phi}_i| \geq 0, \quad (6.94)$$

ここで,  $\Delta$  は次のように定義される.

$$\Delta \equiv I_V - x_n |\tilde{\phi}_n\rangle \langle \tilde{\phi}_n|. \quad (6.95)$$

問題に対する解が存在するという仮定は  $\Delta \geq 0$  であることを意味する. まず,  $\Delta > 0$  の場合を考える. (6.94) 式によって与えられる条件は次のように書き換えられる.

$$I_V - \sum_{i=1}^{n-1} x_i \Delta^{-\frac{1}{2}} |\tilde{\phi}_i\rangle \langle \tilde{\phi}_i| \Delta^{-\frac{1}{2}} \geq 0. \quad (6.96)$$

状態  $\{\Delta^{-\frac{1}{2}}|\tilde{\phi}_i\rangle\}_{i=1}^{n-1}$  は線形独立である。  $V'$  によって、それらの状態で張られた  $(n-1)$  次元部分空間を示す。 次のような  $V'$  での  $n-1$  個の状態の集合を定義する。

$$|\phi'_i\rangle = \frac{Q|\phi_i\rangle}{\sqrt{\langle\phi_i|Q|\phi_i\rangle}} \quad (i = 1, \dots, n-1), \quad (6.97)$$

$$|\tilde{\phi}'_i\rangle = \sqrt{\langle\phi_i|Q|\phi_i\rangle}\Delta^{-\frac{1}{2}}|\tilde{\phi}_i\rangle \quad (i = 1, \dots, n-1), \quad (6.98)$$

ここで、  $Q$  は部分空間  $V'$  上への射影演算子である。  $\langle\tilde{\phi}'_i|\phi'_j\rangle = \delta_{ij}$  という意味では  $\{|\phi'_i\rangle\}_{i=1}^{n-1}$  と  $\{|\tilde{\phi}'_i\rangle\}_{i=1}^{n-1}$  は相反であることを容易に証明することができる。 (6.96) 式によって与えられた条件は次のような形式をとる。

$$I_{V'} - \sum_{i=1}^{n-1} x'_i |\tilde{\phi}'_i\rangle\langle\tilde{\phi}'_i| \geq 0, \quad (6.99)$$

ここで、  $x'_i \equiv x_i / \langle\phi_i|Q|\phi_i\rangle$  である。 また、 最大化する識別成功確率は次のように表すことができる。

$$p = \sum_{i=1}^n \eta_i x_i = \eta_n x_n + N \sum_{i=1}^{n-1} \eta'_i x'_i, \quad (6.100)$$

ここで、  $\eta'_i, N$  は次のように定義される。

$$\eta'_i \equiv \frac{\eta_i \langle\phi_i|Q|\phi_i\rangle}{N},$$

$$N \equiv \sum_{i=1}^{n-1} \eta_i \langle\phi_i|Q|\phi_i\rangle.$$

したがって、 (6.99) 式で与えられた条件の下での (6.100) 式で与えられる  $p$  の最大化と  $x'_i > 0$  は集合  $\{\eta'_i, |\phi'_i\rangle\}_{i=1}^{n-1}$  に対する  $(n-1)$ -state problem と等価である。

次に、  $\Delta$  が特異である場合を考える。 これは  $x_n = 1/\langle\tilde{\phi}_n|\tilde{\phi}_n\rangle$  のときに限り、 起こることと  $\Delta$  は次のような射影演算子であることに気づく。

$$\Delta|\phi_i\rangle = |\phi_i\rangle \quad (i = 1, \dots, n-1), \quad (6.101)$$

$$\Delta|\tilde{\phi}_n\rangle = 0. \quad (6.102)$$

$\langle\tilde{\phi}_n|\tilde{\phi}_i\rangle$  でない限り、  $x_i$  はゼロでなければならないこともわかる。 一般性の損失なしに、 次のような仮定をする。

$$\langle\tilde{\phi}_n|\tilde{\phi}_i\rangle = \begin{cases} 0, & i = 1, \dots, r \\ \text{nonzero}, & i = r+1, \dots, n-1, \end{cases} \quad (6.103)$$

ここで、  $0 \leq r \leq n-1$  である。 もし、  $r = 0$  であるならば、 すべての  $x_i$  はゼロである。 また、  $r \geq 1$  を仮定する。  $V'_r$  は線形独立な状態  $\{|\tilde{\phi}'_i\rangle\}_{i=1}^r$  によって張られる部分空間であるとする。  $V'_r$  は明らかに  $\Delta$  の台集合に含まれるので、 (6.94) 式で与えられた条件は次のように書き換えられる。

$$I_{V'_r} - \sum_{i=1}^r x_i |\tilde{\phi}'_i\rangle\langle\tilde{\phi}'_i| \geq 0. \quad (6.104)$$

一般に, 集合  $\{|\tilde{\phi}_i\rangle\}_{i=1}^r$  と相反である状態は規格化することができない. しかしながら, 係数  $c_i$  を適切に選ぶことで集合  $\{c_i|\tilde{\phi}_i\rangle\}_{i=1}^r$  と相反である規格化された状態の集合  $\{|\phi\rangle_i\}_{i=1}^r$  を得ることは常に可能である. また, 位相因子次第で結果として起こる状態  $|\phi'_i\rangle$  は一意であることに注意しなければならない. したがって, (6.104) 式によって与えられる条件の下で識別成功確率を最大化することと  $x_i \geq 0$  は適切に修正された生起確率  $\eta'_i$  を持つ状態  $\{|\phi'_i\rangle\}_{i=1}^r$  に対する  $r$ -state problem と等価である. ■

## 第7章 3つのqubitのエラーマージンのある識別問題

識別間違い確率に対してエラーマージンを課すことによって minimum-error discrimination と unambiguous discrimination の設定を統一的に扱う識別問題を考察する。Qubit の3つの対称な純粋状態の場合を分析し、最大識別成功確率とそれを実現する最適な測定を解析的に求める。そのとき、最適な測定は3つのタイプに分類され、エラーマージンの値によって3つのうちの1つが最適となる。さらに、qubit の3つの対称な混合状態の場合についても分析する。

### 7.1 問題の定式化

それぞれ生起確率  $\eta_i$  を持つ  $n$  個の量子状態  $\rho_i$  ( $i = 1, 2, \dots, n$ ) のエラーマージンのある識別問題を考察する。測定はPOVMによって記述され、 $n+1$  個の要素  $\{E_0, E_1, E_2, \dots, E_n\}$  から構成される。測定結果が  $i = 1, 2, \dots, n$  であるとき、それは与えられた状態が  $\rho_i$  であると同定することを意味する。そして、 $E_0$  は”わからない”と推定する結果を生み出す。

識別成功確率  $p_o$  と識別間違い確率  $p_\times$  はそれぞれ次のように与えられる。

$$p_o = \sum_{i=1}^n \eta_i \text{tr}[E_i \rho_i], \quad (7.1)$$

$$p_\times = \sum_{i=1}^n \text{tr} \left[ E_i \sum_{j \neq i} \eta_j \rho_j \right]. \quad (7.2)$$

この問題の課題は次のような条件の下で  $p_o$  を最大にすることである。

$$E_\mu \geq 0 \quad (\mu = 0, 1, 2, \dots, n), \quad (7.3a)$$

$$E_0 + \sum_{i=1}^n E_i = I, \quad (7.3b)$$

$$p_\times \leq m, \quad (7.3c)$$

ここで、(7.3a), (7.3b) 式はPOVMの通例の条件である。そして、(7.3c) 式は識別間違い確率がエラーマージン  $m$  ( $0 \leq m \leq 1$ ) を越えてはならないという条件である。

もし,  $m = 0$  ならば, unambiguous discrimination の設定に対応し,  $m = 1$  ならば, minimum-error discrimination の設定に対応する. それゆえ, この識別問題は量子状態の識別問題の 2 つの標準的な設定を連続的に補間する設定である. この最適化問題は SDP(Semidefinite programming) の 1 つとして定式化できることは容易にわかる [37]. また, 参考文献 [38, 39] では, 量子状態の識別問題に対する SDP の応用も見られる.

一方, 次のような条件を満たす Hermite 演算子  $Y$  と実数  $y$  が存在するとする.

$$Y \geq 0, \quad (7.4a)$$

$$Y \geq \eta_i \rho_i - y \sum_{j \neq i} \eta_j \rho_j \quad (i = 1, 2, \dots, n), \quad (7.4b)$$

$$y \geq 0. \quad (7.4c)$$

そのとき, 次のように定義される

$$d \equiv \text{tr}[Y] + my, \quad (7.5)$$

が  $p_\circ$  に対して上限を与える. そして, それは次のように示される.

$$\begin{aligned} p_\circ &= \sum_{i=1}^n \text{tr}[E_i \eta_i \rho_i] \\ &\leq \sum_{i=1}^n \text{tr} \left[ E_i \left( Y + y \sum_{j \neq i} \eta_j \rho_j \right) \right] \\ &= \sum_{i=1}^n \text{tr}[E_i Y] + y p_\times \\ &\leq \text{tr}[Y] + ym = d. \end{aligned}$$

また, この上限は次のような関係が成り立つ場合にのみ実現される.

$$E_i \left[ Y - \eta_i \rho_i + y \sum_{j \neq i} \eta_j \rho_j \right] = 0 \quad (i = 1, 2, \dots, n), \quad (7.6a)$$

$$E_0 Y = 0, \quad (7.6b)$$

$$y(m - p_\times) = 0. \quad (7.6c)$$

以上から, (7.3), (7.4), (7.6) 式で与えられた条件を満たす POVM $\{E_\mu\}$ , 演算子  $Y$ , 実数  $y$  が見つければ, 最適な解を得られることがわかる. (7.4) 式で与えられた条件の下で  $d$  を最小化することを双対問題と呼び, (7.3) 式で与えられた条件の下で  $p_\circ$  を最大化する元の問題を主問題と呼ぶ. また, (7.6) 式で与えられる関係を実現可能条件と呼ぶ.

最適な解を得るための戦略は次の通りである.  $d$  の最小化は (7.4) 式以外の  $Y, y$  に対する仮定を加えることによって実行され, (7.3), (7.6) 式を満たすように POVM $\{E_\mu\}$  も構成される. この方法によって最大識別成功確率とそれを達成する最適な測定を求める. ただし, 双対問題での  $Y, y$  に対する仮定は最適化の厳密性を保証する.

## 7.2 Qubit の 3 つの対称な純粋状態の場合

本節では, qubit の 3 つの対称な純粋状態  $\rho_i = |\phi_i\rangle\langle\phi_i|$  ( $i = 1, 2, 3$ ) の場合を分析する. ここで, 生起確率  $\eta_i$  が等しく, お互いの内積のすべての絶対値が  $|\langle\phi_1|\phi_2\rangle| = |\langle\phi_2|\phi_3\rangle| = |\langle\phi_3|\phi_1\rangle|$  のように等しいことを仮定する. 状態  $\rho_i$  やその他の演算子に対して Bloch ベクトル表示を用いると便利である. それゆえ, 3 つの密度演算子で表される状態  $\rho_i$  は次のように与えられる.

$$\rho_i = \frac{1 + \mathbf{n}_i \cdot \boldsymbol{\sigma}}{2} \quad (i = 1, 2, 3),$$

ここで,  $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$  は Pauli 行列である. Bloch ベクトル  $\mathbf{n}_i$  の互いの内積は次のような関係を満たす.

$$\mathbf{n}_i \cdot \mathbf{n}_j \equiv \begin{cases} 1 & (i = j), \\ \gamma & (i \neq j), \end{cases} \quad (7.7)$$

ここで,  $\gamma$  は qubit の 3 つの対称な純粋状態を特徴づける唯一のパラメータである. そして, それは  $-1/2 \leq \gamma \leq 1$  の範囲にある. さらに,  $Y$  は  $2 \times 2$  Hermite 演算子であるから, 次のように書き換えることができる.

$$Y = \frac{\alpha + \boldsymbol{\beta} \cdot \boldsymbol{\sigma}}{2}.$$

また, (7.4) 式で与えられた条件は次のように定義される

$$\begin{aligned} Y_1 &\equiv Y - \frac{1}{3} [\rho_1 - y(\rho_2 + \rho_3)], \\ Y_2 &\equiv Y - \frac{1}{3} [\rho_2 - y(\rho_1 + \rho_3)], \\ Y_3 &\equiv Y - \frac{1}{3} [\rho_3 - y(\rho_1 + \rho_2)], \end{aligned}$$

と  $Y$  が半正定値演算子であることを意味する. さらに, 演算子  $Y_1, Y_2, Y_3$  は Bloch ベクトル表示を用いると次のように書き換えられる.

$$\begin{aligned} Y_1 &= \frac{1}{2} \left[ \alpha - \frac{1-2y}{3} + (\boldsymbol{\beta} - \mathbf{a}_1) \cdot \boldsymbol{\sigma} \right], \\ Y_2 &= \frac{1}{2} \left[ \alpha - \frac{1-2y}{3} + (\boldsymbol{\beta} - \mathbf{a}_2) \cdot \boldsymbol{\sigma} \right], \\ Y_3 &= \frac{1}{2} \left[ \alpha - \frac{1-2y}{3} + (\boldsymbol{\beta} - \mathbf{a}_3) \cdot \boldsymbol{\sigma} \right], \end{aligned}$$

ここで, 次のように定義される 3 つのベクトル  $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$  を導入した.

$$\mathbf{a}_1 \equiv \frac{1}{3} [\mathbf{n}_1 - y(\mathbf{n}_2 + \mathbf{n}_3)], \quad (7.8)$$

$$\mathbf{a}_2 \equiv \frac{1}{3} [\mathbf{n}_2 - y(\mathbf{n}_1 + \mathbf{n}_3)], \quad (7.9)$$

$$\mathbf{a}_3 \equiv \frac{1}{3} [\mathbf{n}_3 - y(\mathbf{n}_1 + \mathbf{n}_2)]. \quad (7.10)$$

演算子  $Y_1, Y_2, Y_3, Y$  は半正定値演算子であることから、それぞれの小さい方の固有値は正である。それゆえ、 $\alpha$  と  $\beta$  に対する次のような4つの不等式が得られる。

$$\begin{aligned}\alpha &\geq \frac{1-2y}{3} + |\beta - \mathbf{a}_1|, \\ \alpha &\geq \frac{1-2y}{3} + |\beta - \mathbf{a}_2|, \\ \alpha &\geq \frac{1-2y}{3} + |\beta - \mathbf{a}_3|, \\ \alpha &\geq |\beta|.\end{aligned}$$

さらに、 $d$  も次のように書き換えることができる。

$$d = \text{tr} \left[ \frac{\alpha + \beta \cdot \boldsymbol{\sigma}}{2} \right] + ym = \alpha + ym.$$

したがって、双対問題はパラメータ  $\{y, \alpha, \beta\}$  で次のように書き換えることができる。

minimize :

$$d = \alpha + ym, \tag{7.11a}$$

subject to :

$$y \geq 0, \tag{7.11b}$$

$$\alpha \geq \frac{1-2y}{3} + |\beta - \mathbf{a}_1|, \tag{7.11c}$$

$$\alpha \geq \frac{1-2y}{3} + |\beta - \mathbf{a}_2|, \tag{7.11d}$$

$$\alpha \geq \frac{1-2y}{3} + |\beta - \mathbf{a}_3|, \tag{7.11e}$$

$$\alpha \geq |\beta|. \tag{7.11f}$$

初めに、以下で主な結果を述べ、それらの導出は後の小節で詳しく説明する。エラーマージン  $m$  のパラメータ空間は次のような3つの領域に分類される。

$$m_c \leq m \leq 1 \quad (\text{minimum-error 領域}),$$

$$m'_c \leq m \leq m_c \quad (\text{intermediate 領域}),$$

$$0 \leq m \leq m'_c \quad (\text{linear 領域}),$$

ここで、2つの境界エラーマージン  $m_c, m'_c$  は次のように定義される。

$$m_c \equiv \frac{1}{3} \left( 2 - \sqrt{\frac{2(1-\gamma)}{3}} \right), \tag{7.12}$$

$$m'_c \equiv \frac{1}{3} \left( 1 - \sqrt{\frac{1+2\gamma}{3}} \right). \tag{7.13}$$

そして、それぞれの領域の最大識別成功確率は次のように与えられる。

$$p_{\max} = \begin{cases} \frac{1}{3} \left( 1 + \sqrt{\frac{2(1-\gamma)}{3}} \right) & (m_c \leq m \leq 1), \\ \frac{1}{2} \left( m + A + \sqrt{3A(2m - A)} \right) & (m'_c \leq m \leq m_c), \\ 2m & (0 \leq m \leq m'_c), \end{cases} \quad (7.14)$$

ここで、 $A$  は次のような正の定数である。

$$A = \frac{1}{2} \left( 1 - \sqrt{\frac{1+2\gamma}{3}} \right). \quad (7.15)$$

### 7.2.1 Minimum-error 領域

エラーマージンが十分に大きいので、識別間違い確率に対する制限が作用しないとする。そして、それは最適な測定での識別間違い確率  $p_{\times}$  がエラーマージン  $m$  よりも厳密に小さいことを意味する。そのとき、最適な測定は minimum-error discrimination のそれである。今後は、このような場合の領域を minimum-error 領域と呼ぶ。

Minimum-error 領域では、 $p_{\times} < m$  であるから、(7.6c) 式で与えられた条件は  $y = 0$  でなければならないことを意味する。したがって、双対問題は次のように書き換えられる。

minimize :

$$d = \alpha, \quad (7.16a)$$

subject to :

$$\alpha \geq \frac{1}{3} + \left| \beta - \frac{1}{3} \mathbf{n}_1 \right|, \quad (7.16b)$$

$$\alpha \geq \frac{1}{3} + \left| \beta - \frac{1}{3} \mathbf{n}_2 \right|, \quad (7.16c)$$

$$\alpha \geq \frac{1}{3} + \left| \beta - \frac{1}{3} \mathbf{n}_3 \right|. \quad (7.16d)$$

(7.11f) 式で与えられた条件は (7.16b), (7.16c), (7.16d) 式で与えられる条件の結果であるから、除外される。これは次のような不等式から明らかである。

$$\frac{1}{3} + \left| \beta - \frac{1}{3} \mathbf{n}_i \right| \geq |\beta| \quad (i = 1, 2, 3).$$

そして、この関係式は (7.16b), (7.16c), (7.16d) 式の右辺に対して三角不等式を適用することで得られる。

すべての POVM 要素  $E_1, E_2, E_3$  のランクが 1 である解を構成する。したがって、次のように (7.16b), (7.16c), (7.16d) 式で等号が成り立つことを仮定する。

$$\alpha = \frac{1}{3} + \left| \beta - \frac{1}{3} \mathbf{n}_1 \right|, \quad (7.17a)$$



$$\alpha = \frac{1}{3} + \left| \beta - \frac{1}{3} \mathbf{n}_2 \right|, \quad (7.17b)$$

$$\alpha = \frac{1}{3} + \left| \beta - \frac{1}{3} \mathbf{n}_3 \right|. \quad (7.17c)$$

(7.17a), (7.17b), (7.17c) 式を解くことで  $\alpha, \beta$  が得られる. それは次のような方法でわかる. まず, (7.17a), (7.17b), (7.17c) 式から, 次のような 3 つの関係が成り立つ.

$$\begin{aligned} \left| \beta - \frac{1}{3} \mathbf{n}_1 \right| &= \left| \beta - \frac{1}{3} \mathbf{n}_2 \right|, \\ \left| \beta - \frac{1}{3} \mathbf{n}_2 \right| &= \left| \beta - \frac{1}{3} \mathbf{n}_3 \right|, \\ \left| \beta - \frac{1}{3} \mathbf{n}_3 \right| &= \left| \beta - \frac{1}{3} \mathbf{n}_1 \right|. \end{aligned}$$

さらに, これら 3 つの関係から, ベクトル  $\beta$  と 3 つのベクトル  $(\mathbf{n}_1 - \mathbf{n}_2), (\mathbf{n}_2 - \mathbf{n}_3), (\mathbf{n}_3 - \mathbf{n}_1)$  はそれぞれ直交していることがわかる.

$$\begin{aligned} (\mathbf{n}_1 - \mathbf{n}_2) \cdot \beta &= 0, \\ (\mathbf{n}_2 - \mathbf{n}_3) \cdot \beta &= 0, \\ (\mathbf{n}_3 - \mathbf{n}_1) \cdot \beta &= 0. \end{aligned}$$

また, ベクトル  $\beta$  は Bloch ベクトル  $\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3$  の張る空間上にあることから, 次のように表すことができる.

$$\beta = u\mathbf{n}_1 + v\mathbf{n}_2 + w\mathbf{n}_3,$$

ここで,  $u, v, w$  は任意の実数である. この  $\beta$  を上の 3 つの直交関係に代入することで,  $\beta$  の係数  $u, v, w$  には  $u = v = w$  という関係が成り立つことがわかる. したがって, ベクトル  $\beta$  は次のような形式で与えられる.

$$\beta = \frac{1}{3} B (\mathbf{n}_1 + \mathbf{n}_2 + \mathbf{n}_3),$$

ここで,  $B$  は任意の実数である. 次に, この  $\beta$  を (7.17a), (7.17b), (7.17c) 式にそれぞれ代入することで, 次のような  $\alpha$  と  $B$  に対する同一の関係が得られる.

$$\alpha = \frac{1}{3} \left( 1 + \sqrt{3(1+2\gamma)B^2 - 2(1+2\gamma)B + 1} \right).$$

今,  $\alpha$  を最小にする  $B$  を決定するために, 次のような関数  $f(B)$  を定義する.

$$f(B) = 3(1+2\gamma)B^2 - 2(1+2\gamma)B + 1.$$

これは  $B$  に対する下に凸の 2 次関数であることは明らかである. それゆえ,  $B = 1/3$  のとき, 最小値  $2(1-\gamma)/3$  をとることがわかる.

したがって、ベクトル  $\beta$  は次のように与えられる。

$$\beta = \frac{1}{9} (\mathbf{n}_1 + \mathbf{n}_2 + \mathbf{n}_3). \quad (7.18)$$

そして、 $\alpha$  は次のように得られる。

$$\alpha = d = \frac{1}{3} \left( 1 + \sqrt{\frac{2(1-\gamma)}{3}} \right). \quad (7.19)$$

(7.19) 式で与えられた上限  $d$  を達成する POVM  $\{E_\mu\}$  を構成する。結論の出ない結果に対する要素  $E_0$  はこの領域ではゼロである。そして、それは (7.6b) 式で与えられる実現可能条件を満たす。(7.6a) 式で与えられた実現可能条件は POVM 要素  $E_1, E_2, E_3$  が次のような形式をとることを要請する。

$$E_i = C_i \frac{1 - \mathbf{e}_i \cdot \boldsymbol{\sigma}}{2} \quad (i = 1, 2, 3),$$

ここで、次のような 3 つのベクトルを定義した。

$$\mathbf{e}_i \equiv \frac{\beta - \frac{1}{3}\mathbf{n}_i}{\left| \beta - \frac{1}{3}\mathbf{n}_i \right|} \quad (i = 1, 2, 3),$$

ただし、ベクトル  $\beta$  は (7.18) 式で与えられている。

(7.3a), (7.3b), (7.3c) 式で与えられた条件を満たすように係数  $C_i$  ( $i = 1, 2, 3$ ) を決定する。(7.3b) 式で与えられた POVM の完全性関係から、係数  $C_i$  に対する次のような 2 つの関係が得られる。

$$\frac{1}{2} (C_1 + C_2 + C_3) = 1, \quad (7.20)$$

$$C_1 \mathbf{e}_1 + C_2 \mathbf{e}_2 + C_3 \mathbf{e}_3 = 0. \quad (7.21)$$

(7.21) 式では、3 つのベクトル  $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$  のそれぞれは Bloch ベクトル  $\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3$  で表せられる。Bloch ベクトル  $\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3$  の線形独立性から、 $C_1 = C_2 = C_3$  であることがわかる。それゆえ、係数  $C_i$  ( $i = 1, 2, 3$ ) は次のように与えられる。

$$C_1 = C_2 = C_3 = \frac{2}{3}.$$

さらに、 $C_i > 0$  であるから、POVM  $\{E_1, E_2, E_3\}$  は (7.3a) 式を満たす。

(7.3c) 式で与えられた残りの条件によって、次のような関係が成り立つことがわかる。

$$p_{\times} = \frac{1}{3} \left( 2 - \sqrt{\frac{2(1-\gamma)}{3}} \right) \leq m, \quad (7.22)$$

ここで、識別間違い確率  $p_{\times}$  は上で構成された POVM を用いて計算された。

したがって、もし、エラーマージン  $m$  が  $m_c \leq m \leq 1$  の範囲にあるならば、(7.19) 式で与えられた上限は達成され、最大識別成功確率は次のように与えられる。

$$p_{\max} = \frac{1}{3} \left( 1 + \sqrt{\frac{2(1-\gamma)}{3}} \right). \quad (7.23)$$

## 7.2.2 Linear 領域と intermediate 領域

この小節では, すべての POVM 要素  $E_1, E_2, E_3, E_0$  がゼロではない解を構成する. (7.6a), (7.6b) 式で与えられた実現可能条件は演算子  $Y_1, Y_2, Y_3, Y$  のランクが多くても 1 であることを意味する. すなわち, 演算子  $Y_1, Y_2, Y_3, Y$  の小さい方の固有値がすべてゼロである. したがって, 次のように (7.11c), (7.11d), (7.11e), (7.11f) 式で等号が成り立つことを仮定する.

$$\alpha = \frac{1-2y}{3} + |\beta - \mathbf{a}_1|, \quad (7.24a)$$

$$\alpha = \frac{1-2y}{3} + |\beta - \mathbf{a}_2|, \quad (7.24b)$$

$$\alpha = \frac{1-2y}{3} + |\beta - \mathbf{a}_3|, \quad (7.24c)$$

$$\alpha = |\beta|. \quad (7.24d)$$

(7.24d) 式を用いて, (7.24a), (7.24b), (7.24c) 式から  $\alpha$  を消去し, ベクトル  $\beta$  に対する 3 つの方程式に書き換えることができる.

$$|\beta| = \frac{1-2y}{3} + |\beta - \mathbf{a}_1|, \quad (7.25a)$$

$$|\beta| = \frac{1-2y}{3} + |\beta - \mathbf{a}_2|, \quad (7.25b)$$

$$|\beta| = \frac{1-2y}{3} + |\beta - \mathbf{a}_3|. \quad (7.25c)$$

計算は少し複雑になるが, Minimum-error 領域のときと同様の議論で, ベクトル  $\beta$  は次のような形式で与えられることがわかる.

$$\beta = \frac{1}{3}B(\mathbf{n}_1 + \mathbf{n}_2 + \mathbf{n}_3),$$

ここで,  $B$  は任意の実数である. また,  $\alpha - (1-2y)/3 \geq 0$  であることに注意しなければならない. この  $\beta$  を (7.25a), (7.25b), (7.25c) 式それぞれに代入し,  $B$  について解くことで, 次のような  $B$  が得られる.

$$B = \frac{1}{2} \left( 1 \pm \sqrt{\frac{3}{1+2\gamma}} \right) \frac{(y-2)y}{1-2y}.$$

したがって, ベクトル  $\beta$  は次のように与えられる.

$$\beta = \frac{1}{2} \left( 1 \pm \sqrt{\frac{3}{1+2\gamma}} \right) \frac{(y-2)y}{1-2y} \left( \frac{\mathbf{n}_1 + \mathbf{n}_2 + \mathbf{n}_3}{3} \right). \quad (7.26)$$

そして,  $\alpha$  は次のように得られる.

$$\alpha = |\beta| = \frac{1}{2} \left( 1 \pm \sqrt{\frac{1+2\gamma}{3}} \right) \frac{(y-2)y}{1-2y} \quad (7.27)$$

ただし,  $\alpha - (1 - 2y)/3 \geq 0$  であった. それゆえ, パラメータ  $y$  の許される範囲は  $1/2 \leq y \leq 2$  であることがわかる. 以上から, 識別成功確率に対する上限はパラメータ  $y$  の関数として次のように与えられる.

$$d = \alpha + ym = \frac{1}{2} \left( 1 \pm \sqrt{\frac{1 + 2\gamma}{3}} \right) \frac{(y - 2)y}{1 - 2y} + my. \quad (7.28)$$

上の方程式での複号について, より小さい上限を得るために負の符号をとる. それに対応して, 今後, (7.26), (7.27) 式の複号でも負の符号をとる.

今, 上限  $d$  が最小であるようにパラメータ  $y$  を決定する. そこで, 上限  $d$  がパラメータ  $y$  の許される範囲  $1/2 \leq y \leq 2$  でどのように変化するかを見てみる. まず,  $d$  を  $y$  に関して微分すると,

$$\frac{\partial}{\partial y} d = m - \frac{1}{2}A - \frac{3}{2}A \frac{1}{(2y - 1)^2},$$

である. ここで,  $A$  は (7.15) 式によって定義された正の定数である. もし, エラーマージン  $m$  が  $m < A/2$  であるならば, 上限  $d$  はパラメータ  $y$  に関する単調減少の関数であることがわかる. それゆえ, この場合では,  $d$  は  $y = 2$  で最小値  $d_{\min} = 2m$  をとる. 他方,  $A/2 \leq m$  の場合,  $\frac{\partial}{\partial y} d = 0$  として生み出されたパラメータ  $y$  に対する 2 次方程式は次のような 2 つの根  $y_e$  を持つ.

$$y_e = \frac{1}{2} \left( 1 \pm \sqrt{\frac{3A}{2m - A}} \right). \quad (7.29)$$

根  $y_e$  の複号について,  $1/2 \leq y \leq 2$  であるから, 正の符号をとる.

ここで, 2 つの場合が考えられる. 1 つは  $y_e \geq 2$  の場合である. そして, それはエラーマージン  $m$  の範囲として次のように書き換えられる.

$$m \leq \frac{2}{3}A \equiv m'_c, \quad (7.30)$$

ここで, 右辺の  $m'_c$  は (7.13) 式で定義されている. さらに, この領域を linear 領域と呼ぶ. Linear 領域では, 上限  $d$  は  $y = 2$  で最小である. また,  $\alpha, \beta$  は共にゼロとなるので,  $Y = 0$  である. それゆえ, linear 領域での上限は次のように与えられる.

$$d = 2m. \quad (7.31)$$

そして, それはエラーマージン  $m$  に関して線形である.

一方,  $y_e < 2$  の場合では, エラーマージン  $m$  の範囲は次のように得られる.

$$m'_c \equiv \frac{2}{3}A < m. \quad (7.32)$$

この領域を intermediate 領域と呼ぶ. Intermediate 領域では, 上限  $d$  は  $y = y_e$  で最小である. 識別成功確率に対する上限を最小にする  $Y$  と  $y$  を用いて  $d = \text{tr}[Y] + ym$  を計算することで, 次のような上限が得られる.

$$d = \frac{1}{2} \left( m + A + \sqrt{3A(2m - A)} \right). \quad (7.33)$$

次の小節では, 得られたそれぞれの領域の上限を達成する最適な POVM を構成する.

## A. Linear 領域

Linear 領域では,  $\alpha = \beta = 0$  であるから,  $Y = 0$  である. これは (7.6b) 式で与えられた実現可能条件が POVM 要素  $E_0$  に対して何の制限も与えないことを示す. また, (7.6a) 式で与えられた実現可能条件は POVM 要素が次のような形式をとることを要請する.

$$E_i = C \frac{1 + \mathbf{e}_i \cdot \boldsymbol{\sigma}}{2} \quad (i = 1, 2, 3).$$

ここで, 係数  $C$  は指数  $i$  によらないことを仮定した. そして, ベクトル  $\mathbf{e}_i$  は次のように定義される.

$$\mathbf{e}_i \equiv \mathbf{a}_i \quad (i = 1, 2, 3),$$

ただし, この  $\mathbf{a}_i$  は (7.8), (7.9), (7.10) 式で与えられた  $\mathbf{a}_i$  ( $i = 1, 2, 3$ ) に  $y = 2$  を代入したものである.

問題は集合  $\{E_1, E_2, E_3\}$  が (7.3a), (7.3b), (7.3c), (7.6c) 式で与えられた条件を満たすように係数  $C$  を選ぶことができるかどうかである. まず, (7.3c), (7.6c) 式は  $y = 2$  であるから,  $p_{\times} = m$  と変換できる. 上で構成した POVM を用いて  $p_{\times}$  を計算することで, 係数  $C$  が次のように与えられることがわかる.

$$C = \frac{3m}{1 - \gamma}.$$

そして,  $C$  は  $-1/2 \leq \gamma \leq 1$  であるから, 正であることは明らかである. それゆえ, POVM 要素  $E_1, E_2, E_3$  は (7.3a) 式を満たす. さらに, 結論の出ない結果を示す POVM 要素  $E_0$  は (7.3b) 式で与えられる POVM の完全性関係から次のように得られる.

$$\begin{aligned} E_0 &= I - (E_1 + E_2 + E_3) \\ &= 1 - \frac{9m}{2(1 - \gamma)} + \frac{3m}{2(1 - \gamma)} (\mathbf{n}_1 + \mathbf{n}_2 + \mathbf{n}_3) \cdot \boldsymbol{\sigma}. \end{aligned} \quad (7.34)$$

ここで, POVM 要素  $E_0$  が (7.3a) 式を満たすためには, 次のように与えられる  $E_0$  の小さい方の固有値  $\lambda_-$  が正でなければならない.

$$\lambda_- = 1 - \frac{9}{2(1 - \gamma)} \left( 1 + \sqrt{\frac{1 + 2\gamma}{3}} \right) m.$$

これはエラーマージン  $m$  が  $0 \leq m \leq m'_c$  の範囲にあることから, 満たされる.

したがって, もし, エラーマージン  $m$  が  $0 \leq m \leq m'_c$  の範囲にあるならば, (7.31) 式で与えられた上限は達成される. そして, 最大識別成功確率は次のように与えられる.

$$p_{\max} = 2m. \quad (7.35)$$

## B. Intermediate 領域

(7.33) 式で与えられた上限  $d$  を達成する POVM  $\{E_0, E_1, E_2, E_3\}$  を構成する.

$$E_\mu = C_\mu \frac{1 + \mathbf{e}_\mu \cdot \boldsymbol{\sigma}}{2} \quad (\mu = 0, 1, 2, 3),$$

ここで,  $\mathbf{e}_\mu$  は次のように定義される.

$$\mathbf{e}_0 \equiv \frac{\boldsymbol{\beta}}{|\boldsymbol{\beta}|}, \quad \mathbf{e}_i \equiv \frac{\boldsymbol{\beta} - \mathbf{a}_i}{|\boldsymbol{\beta} - \mathbf{a}_i|} \quad (i = 1, 2, 3).$$

ただし,  $\boldsymbol{\beta}$  は (7.26) 式で与えられた  $\boldsymbol{\beta}$  の  $y$  に対して (7.29) 式で与えられた  $y_e$  を代入したもので,  $\mathbf{a}_i$  は (7.8), (7.9), (7.10) 式で与えられた  $\mathbf{a}_i$  ( $i = 1, 2, 3$ ) に  $y = y_e$  を代入したものである.

今, (7.3b) 式で与えられた POVM の完全性関係から, 係数  $C_\mu$  に対する 2 つの関係が得られる.

$$\frac{1}{2}(C_0 + C_1 + C_2 + C_3) = 1, \quad (7.36)$$

$$C_0 \mathbf{e}_0 + C_1 \mathbf{e}_1 + C_2 \mathbf{e}_2 + C_3 \mathbf{e}_3 = 0. \quad (7.37)$$

(7.37) 式で, 4 つのベクトル  $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_0$  は Bloch ベクトル  $\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3$  によって表せられる. Bloch ベクトルの線形独立性から,  $C_1 = C_2 = C_3$  という関係があることがわかる. それゆえ, 今後は  $C_i$  ( $i = 1, 2, 3$ ) を  $C$  とする. したがって, (7.36), (7.37) 式から, 係数  $C$  および  $C_0$  は次のように与えられる.

$$\begin{aligned} C &= \frac{A}{1-\gamma} \left[ 2 + 3(m - A) + \sqrt{3A(2m - A)} \right], \\ C_0 &= 2 - 3C. \end{aligned}$$

POVM 要素  $E_1, E_2, E_3, E_0$  が (7.3a) 式を満たすためには, 係数  $C$  および  $C_0$  は正でなければならない. これはエラーマージン  $m$  が  $m'_c \leq m \leq m_c$  の範囲にあることから, 満たされる.

残りの条件は (7.3c), (7.6c) 式である. そして, それは  $1/2 \leq y \leq 2$  であることから,  $p_\times = m$  と変換される. 上で構成された POVM を用いて計算することで,  $p_\times = m$  が成り立つことを明確に証明することができる. これは偶然の一致ではなく, パラメータ  $y$  をどのように決定したかの結果である. パラメータ  $y$  は上限  $d$  を最小にするように決定された. つまり, 次のような方程式を解くことで得られた.

$$\frac{\partial}{\partial y} d = \frac{\partial}{\partial y} \text{tr}[Y] + m = 0.$$

ここで, 4.2 節で与えられた議論を用いると,  $\frac{\partial}{\partial y} \text{tr}[Y] = -p_\times$  は示することができる. そして, それは  $d$  の最小化が  $p_\times = m$  という関係を導くことを意味する.

したがって, もし, エラーマージン  $m$  が  $m'_c \leq m \leq m_c$  の範囲にあるならば, (7.33) 式で与えられた上限は達成され, 最大識別成功確率は次のように与えられる.

$$p_{\max} = \frac{1}{2} \left( m + A + \sqrt{3A(2m - A)} \right). \quad (7.38)$$

### 7.2.3 例

次のような Bloch ベクトル  $\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3$  で定義される状態の集合を考える.

$$\mathbf{n}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{n}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad \mathbf{n}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Bloch ベクトルのお互いの内積は  $\gamma = \mathbf{n}_i \cdot \mathbf{n}_j = 0$  ( $i \neq j$ ) で与えられる.

図 7.1 はエラーマージン  $m$  の関数として最大識別成功確率  $p_{\max}$  と結論の出ない結果を生む確率  $p_?$  を表示する. エラーマージンが 0 から 1 まで増えるにつれて, 最適な測定の種類は次のような方法で変化する. まず,  $m = m'_c$  で linear 領域のタイプから intermediate 領域のタイプに変化する. そして, 次に,  $m = m_c$  で minimum-error 領域のタイプに変化する. 範囲  $m_c \leq m \leq 1$  では, 最大識別成功確率  $p_{\max}$  と結論の出ない結果を生む確率  $p_?$  はエラーマージン  $m$  に依存しない. また,  $p_{\max}$  と  $p_?$  のカーブは minimum-error 領域と intermediate 領域の境界を明らかに示すが,  $m = m'_c$  ではカーブはほとんど滑らかである.

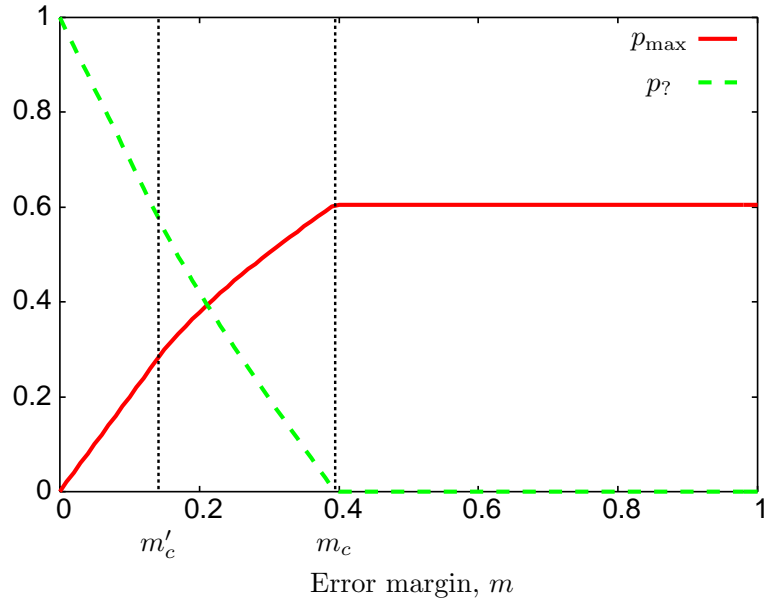


図 7.1: エラーマージン  $m$  に対する最大識別成功確率  $p_{\max}$  と結論の出ない結果を生む確率  $p_?$

第 4 章で, 一般の生起確率を持つ 2 つの純粋状態のエラーマージンのある識別問題を分析し, エラーマージンが十分に小さければ, 識別される状態の 1 つを除外するのが最適である領域があることがわかっている. しかしながら, 今節で考えた対称な状態に対してそのような領域はなく, 状態の置き換えに関して対称性がある.

### 7.3 Qubit の 3 つの対称な混合状態の場合

今節では、識別される 3 つの状態  $\rho_1, \rho_2, \rho_3$  が次のような条件を満たす対称な混合状態である場合を考える。

$$\text{tr} [\rho_1^2] = \text{tr} [\rho_2^2] = \text{tr} [\rho_3^2] < 1, \quad \text{tr} [\rho_1 \rho_2] = \text{tr} [\rho_2 \rho_3] = \text{tr} [\rho_3 \rho_1].$$

また、Bloch ベクトルのお互いの内積は次のようにパラメータ化される。

$$\mathbf{n}_i \cdot \mathbf{n}_j \equiv \begin{cases} r & (i = j), \\ \gamma & (i \neq j), \end{cases} \quad (7.39)$$

ここで、 $0 \leq r \leq 1$ ,  $-r/2 \leq \gamma \leq r$  である。このように qubit の 3 つの混合状態の対称な集合は 2 つのパラメータ  $r, \gamma$  によって特徴づけられる。

問題は 7.2 節での (7.11) 式と全く同じ方法で定式化される。計算はより複雑になるが、最適解は純粋状態の場合のように得ることができる。

以下で、qubit の 3 つの対称な混合状態の場合の結果を述べる。表現をより簡単にするために、次のような  $s, t$  を定義する。

$$s \equiv 1 - r, \quad (7.40)$$

$$t \equiv 1 - \gamma. \quad (7.41)$$

Qubit の 3 つの対称な混合状態の場合の最大識別成功確率は次のように与えられる。

$$p_{\max} = \begin{cases} \frac{1}{3} \left( 1 + \sqrt{\frac{2(t-s)}{3}} \right) & (m_c \leq m \leq 1), \\ \frac{1}{s+2t} \left[ \frac{1}{2} m (s+2t) + A (t-s) + \sqrt{3A (t-s) [m (s+2t) - A (s+t)]} \right] & (m'_c \leq m \leq m_c), \\ \frac{1}{s+t} \left( t + \sqrt{\frac{(t-s)(s+2t)}{2}} \right) m & (0 \leq m \leq m'_c), \end{cases} \quad (7.42)$$

ここで、 $A$  は次のように定義される。

$$A \equiv \frac{1}{2} \left( 1 - \sqrt{\frac{r+2\gamma}{3}} \right). \quad (7.43)$$

さらに、2 つの境界エラーマージン  $m_c, m'_c$  は次のように与えられる。

$$m_c \equiv \frac{1}{3} \left( 2 - \sqrt{\frac{2(t-s)}{3}} \right), \quad (7.44)$$

$$m'_c \equiv \frac{2}{3} \left( 2 - \sqrt{\frac{2(t-s)}{s+2t}} \right) A. \quad (7.45)$$

ただし、 $r = 1$  のとき、これは 7.2 節で得られた結果を再現している。



## 第8章 結論

本研究では、量子情報分野の中でも、最も基本的で重要な研究課題である量子状態の識別問題について考察し、量子状態の識別問題を考える上で標準的な設定である minimum-error discrimination や unambiguous discrimination、識別間違い確率に対してエラーマージンを導入することで minimum-error discrimination と unambiguous discrimination を連続的に補間する設定での識別問題を分析した。以下に、本研究で新しく得られた結果をまとめる。

まず、第4章で、一般の生起確率を持つ2つの純粋状態のエラーマージンのある識別問題を考察し、最大識別成功確率を導出した。そこで、最適な測定は3つのタイプに分類され、そのタイプによって生起確率とエラーマージンの2次元パラメータ空間が次のような3つの領域に分けられることがわかった。

$$\begin{aligned} m_c \leq m \leq 1 & \quad (\text{minimum-error 領域}), \\ m'_c \leq m \leq m_c & \quad (\text{intermediate 領域}), \\ 0 \leq m \leq m'_c & \quad (\text{single-state 領域}). \end{aligned}$$

さらに、エラーマージンには、平均の間違い確率に対する弱いエラーマージン条件と条件付き間違い確率に対する強いエラーマージン条件という2つの制限のタイプが考えられた。そこで、この2つの制限のタイプの識別成功確率のあいだにある関係を証明した。これにより、2つの純粋状態の場合では、どのような場合でも解析的な形式で最大識別成功確率が得られるようになった。

次に、識別される状態の数が3つになった場合を考察した。識別される状態が2つ以上の複数である場合、識別問題の標準的な設定である minimum-error discrimination や unambiguous discrimination でさえ、特別な場合を除いて、完全に解析的な解は得られていなかった。それは識別される状態の数が増えることにより決定しなければならないパラメータの数も増えるので、問題自体がより複雑になることが原因として考えられた。そこで、本研究では、主問題を直接解くのではなく、そこから導かれた双対問題を解くことを提案した。まず、第5章では、qubit の3つの純粋状態の minimum-error discrimination を分析した。そして、生起確率が等しい場合に最大識別成功確率とそれを達成する最適な POVM を構成することができた。そこで、識別される状態の Bloch ベクトルの終点が成す三角形の外心が最適な解を構成するための重要な役割を果たすことを証明した。そして、最適な測定は識別される状態の Bloch ベクトルの成す三角形が鋭角三角形または直角三角形の場合と鈍角三角形の場合とで分類されることがわかった。さらに、一般の生起確率の場合への拡張を試みたが、現時点では、完全に解析解を得ることはできなかった。次に、第6章では、3つの純粋状態の unambiguous discrimination を分析した。まず、SDP (Semidefinite programming) として、 $n$  個の線形独立な純粋状態

の unambiguous discrimination を定式化し、一般的な性質や解が一意であることなどを証明した。さらに、unambiguous discrimination での最適な戦略では、与えられた状態がいくつかの状態である同定する確率が 0 であることがあった。そこで、この確率をうまく扱うために変数に対するある制限を緩和した問題を考えると非常に便利であることを示した。そして、これらの戦略を 3 つの純粋状態の場合に適用し、互いの内積が実数である場合の解析解が得られた。互いの内積が一般の複素数の場合への拡張も試みたが、ある特別な場合にしか解析解は得られなかった。また、ここで用いた戦略を 3 つの純粋状態のエラーマージンのある識別問題や 3 つのユニタリープロセスの識別などへ拡張することで今後の研究への興味を持つことができるだろう。第 7 章では、qubit の 3 つの対称な純粋状態のエラーマージンのある識別問題を分析し、完全に解析的な形式で最大識別成功確率とそれを実現する最適な POVM を構成した。さらに、この方法が qubit の 3 つの対称な混合状態の場合にも適用できることを示した。そこで、最適な測定はエラーマージンによって 3 つのタイプに分類されることがわかった。また、この分類は次のように”わからない”という結果を表す POVM 要素  $E_0$  のランクによってもなされることがわかった。

$$\text{rank}(E_0) = \begin{cases} 0 & (\text{minimum-error 領域}) \\ 1 & (\text{intermediate 領域}) \\ 2 & (\text{linear 領域}) \end{cases}$$

$\text{rank}(E_0) = 0$  のとき、最適な測定は minimum-error 領域のそれである。そして、 $\text{rank}(E_0) = 1$  のとき、最適な測定は intermediate 領域のそれであり、 $\text{rank}(E_0) = 2$  のとき、最適な測定は linear 領域のそれである。しかしながら、 $\text{rank}(E_0) = 1$  の場合と  $\text{rank}(E_0) = 2$  の場合の物理的意味の違いについては明確ではない。

本研究により、2 つの純粋状態の場合についてはどのような場合でも解析的な形式で最大識別成功確率を得られるようになった。そして、3 つの純粋状態の場合についても、標準的な設定である minimum-error discrimination や unambiguous discrimination、そして、それら 2 つの設定を統一的に扱えるエラーマージンのある識別問題で解析的な形式で最大識別成功確率を得ることができた。しかしながら、3 つの純粋状態の場合については、minimum-error discrimination や unambiguous discrimination でさえ、特別な場合でしか解析解を得ることはできなかった。今後の課題として、3 つの純粋状態のより一般的な場合について、それぞれの設定で解析解を求めることが挙げられる。さらに、識別される状態の数を 3 つ以上の複数である識別問題がどうなるかということも考えられる。

# 謝辞

本論文を作成するにあたり、指導教官である林明久教授には最初から最後まで懇切丁寧なご指導を賜り、感謝の念に堪えません。堀邊稔教授、橋本貴明教授にも様々なご指導、ご助言頂きましたことを厚く御礼申し上げます。また、田嶋直樹准教授には日頃より丁寧なご指導、お世話頂き、誠にありがとうございました。

最後になりましたが、学部生の頃より9年間という長きに渡り、お世話になりました物理工学科ならびに物理工学専攻の先生方にも厚く御礼申し上げ、謝辞の言葉とさせていただきます。

2013年3月

杉本 宏行

## 参考文献

- [1] A. Chefles, Contemp. Phys. **41**, 401 (2000).
- [2] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
- [3] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
- [4] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
- [5] D. Dieks, Phys. Lett. A **126**, 303 (1988).
- [6] A. Peres, Phys. Lett. A **128**, 19 (1988).
- [7] G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).
- [8] R. B. M. Clarke, A. Chefles, S. M. Barnett, and E. Riis, Phys. Rev. A **63**, 040305 (2001).
- [9] S. Croke, E. Andersson, S. M. Barnett, C. R. Gilson, and J. Jeffers, Phys. Rev. Lett. **96**, 070401 (2006).
- [10] O. Jimenez, M. A. Solis-Prosser, A. Delgado, and L. Neves, Phys. Rev. A **84**, 062315 (2011).
- [11] U. Herzog, Phys. Rev. A **85**, 032312 (2012).
- [12] A. Chefles and S. M. Barnett, J. Mod. Opt. **45**, 1295 (1998).
- [13] C. -W. Zhang, C. -F. Li, and G. -C. Guo, Phys. Lett. A **261**, 25 (1999).
- [14] J. Fiurasek and M. Jezek, Phys. Rev. A **67**, 012321 (2003).
- [15] Y. C. Eldar, Phys. Rev. A **67**, 042309 (2003).
- [16] M. A. P. Touzel, R. B. A. Adamson, and A. M. Steinberg, Phys. Rev. A **76**, 062314 (2007).
- [17] A. Hayashi, T. Hashimoto, and M. Horibe, Phys. Rev. A **78**, 012333 (2008).
- [18] H. Sugimoto, T. Hashimoto, M. Horibe, and A. Hayashi, Phys. Rev. A **80**, 052322 (2009).

- [19] E. Andersson, S. M. Barnett, C. R. Gilson, and K. Hunter, Phys. Rev. A **65**, 052308 (2002).
- [20] K. Hunter, AIP Conf. Proc. **734**, 83 (2004).
- [21] S. M. Barnett and S. Croke, J. Phys. A: Math. Theor. **42**, 062001 (2009).
- [22] B. F. Samsonov, Phys. Rev. A **80**, 052305 (2009).
- [23] A. Assalini, G. Cariolaro, and G. Pierobon, Phys. Rev. A **81**, 012315 (2010).
- [24] A. Chefles, Phys. Lett. A **239**, 339 (1998).
- [25] A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).
- [26] A. Peres and D. Terno, J. Phys. A **31**, 7105 (1998).
- [27] Y. Sun, M. Hillery, and J. A. Bergou, Phys. Rev. A **64**, 022311 (2001).
- [28] S. Zhang, Y. Feng, X. Sun, and M. Ying, Phys. Rev. A **64**, 062103 (2001).
- [29] M. A. Jafarizadeh, M. Rezaei, N. Karimi, and A. R. Amiri, Phys. Rev. A **77**, 042314 (2008).
- [30] B. F. Samsonov, Phys. Rev. A **79**, 042312 (2009).
- [31] S. Pang and S. Wu, Phys. Rev. A **80**, 052320 (2009).
- [32] Y. Taninaka, H. Sugimoto, and A. Hayashi, unpublished.
- [33] H. Sugimoto, T. Hashimoto, M. Horibe, and A. Hayashi, Phys. Rev. A **82**, 032338 (2010).
- [34] H. Sugimoto, Y. Taninaka, and A. Hayashi, Phys. Rev. A **86**, 042311 (2012).
- [35] E. Bagan, R. Munoz-Tapia, G. A. Olivares-Renteria, and J. A. Bergou, arXiv:1206.4145 [quant-ph].
- [36] U. Herzog, Phys. Rev. A **86**, 032314 (2012).
- [37] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 49 (1996).
- [38] Y. C. Eldar, A. Megretski, and G. C. Verghese, IEEE Trans. Inf. Theory **49**, 1007 (2003).
- [39] Y. C. Eldar, IEEE Trans. Inf. Theory **49**, 446 (2003).
- [40] M. Yamashita, K. Fujisawa, and M. Kojima, Optim. Meth. Softw. **18**, 491 (2003).
- [41] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

- [42] T. Rudolph, R. W. Spekkens, and P. S. Turner, Phys. Rev. A **68**, 010301(R) (2003).
- [43] Y. Feng, R. Duan, and M. Ying, Phys. Rev. A **70**, 012308 (2004).
- [44] U. Herzog and J. A. Bergou, Phys. Rev. A **71**, 050301(R) (2005).
- [45] P. Raynal and N. Lütkenhaus, Phys. Rev. A **72**, 022342 (2005).
- [46] X. -F. Zhou, Y. -S. Zhang, and G. -C. Guo, Phys. Rev. A **75**, 052314 (2007).
- [47] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).
- [48] T. Hashimoto, A. Hayashi, M. Hayashi, and M. Horibe, Phys. Rev. A **81**, 062327 (2010).

## 付 録 A Pauli 行列

量子情報分野において, Pauli 行列は非常に有用である. そして, Pauli 行列は次のような  $2 \times 2$  行列で定義される.

$$\sigma_x \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

ここで, 単位行列  $I$  を含めた 4 つの行列を Pauli 行列と呼ぶこともある.

Pauli 行列は Hermite であり, Unitary でもある. そして, 以下のような性質を持つ. まず,  $\sigma_x, \sigma_y, \sigma_z$  のトレースおよび行列式は次のように与えられる.

$$\begin{aligned} \text{tr} [\sigma_x] &= \text{tr} [\sigma_y] = \text{tr} [\sigma_z] = 0, \\ \det [\sigma_x] &= \det [\sigma_y] = \det [\sigma_z] = -1. \end{aligned}$$

また, 単位行列  $I$  のトレースおよび行列式はそれぞれ  $\text{tr} [I] = 2, \det [I] = 1$  である.

次に, Pauli 行列の積はそれぞれ次のように与えられる.

$$\begin{aligned} \sigma_x^2 &= \sigma_y^2 = \sigma_z^2 = I, \\ \sigma_x \sigma_y &= -\sigma_y \sigma_x = i\sigma_z, \\ \sigma_y \sigma_z &= -\sigma_z \sigma_y = i\sigma_x, \\ \sigma_z \sigma_x &= -\sigma_x \sigma_z = i\sigma_y. \end{aligned}$$

したがって, 次のような交換関係が成り立つことは明らかである.

$$\begin{aligned} [\sigma_x, \sigma_y] &= 2i\sigma_z, \quad [\sigma_y, \sigma_z] = 2i\sigma_x, \quad [\sigma_z, \sigma_x] = 2i\sigma_y, \\ [\sigma_y, \sigma_x] &= -2i\sigma_z, \quad [\sigma_z, \sigma_y] = -2i\sigma_x, \quad [\sigma_x, \sigma_z] = -2i\sigma_y. \end{aligned}$$

そして, 次のような反交換関係も成り立つ.

$$\begin{aligned} \{\sigma_x, \sigma_x\} &= \{\sigma_y, \sigma_y\} = \{\sigma_z, \sigma_z\} = 2I, \\ \{\sigma_x, \sigma_y\} &= \{\sigma_x, \sigma_z\} = \{\sigma_y, \sigma_x\} = \{\sigma_y, \sigma_z\} = \{\sigma_z, \sigma_x\} = \{\sigma_z, \sigma_y\} = 0. \end{aligned}$$

さらに, 次のような関係も成り立つ.

$$(\mathbf{a} \cdot \boldsymbol{\sigma})(\mathbf{b} \cdot \boldsymbol{\sigma}) = (\mathbf{a} \cdot \mathbf{b})I + i(\mathbf{a} \times \mathbf{b}) \cdot \boldsymbol{\sigma},$$

ここで,  $\mathbf{a}, \mathbf{b}$  は任意の 3 次元ベクトルである.

最後に、任意の  $2 \times 2$  Hermite 行列は Pauli 行列の線形結合によって表すことができる。そして、それは次のように示される。まず、任意の  $2 \times 2$  Hermite 行列  $A$  およびその Hermite 共役 (転置複素共役)  $A^\dagger$  を次のように定義する。

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad A^\dagger = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix}. \quad (\text{A.1})$$

$A$  は Hermite であることから、次のような関係が成り立つ。

$$A = A^\dagger.$$

これは各行列要素に対して、次のような関係が成り立つことを意味する。

$$a = a^*, \quad b = c^*, \quad c = b^*, \quad d = d^*.$$

それゆえ、 $a, d$  は実数であり、 $b, c$  は次のような複素数で与えられる。

$$b = x - iy, \quad c = x + iy,$$

ここで、 $x, y$  は実数である。したがって、 $A$  は次のように書き換えられる。

$$\begin{aligned} A &= \begin{pmatrix} a & x - iy \\ x + iy & d \end{pmatrix} \\ &= \frac{a+d}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + x \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + y \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + \frac{a-d}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \alpha + \beta_x \sigma_x + \beta_y \sigma_y + \beta_z \sigma_z = \alpha + \boldsymbol{\beta} \cdot \boldsymbol{\sigma}, \end{aligned} \quad (\text{A.2})$$

ここで、次のような実数  $\alpha, \beta_x, \beta_y, \beta_z$  を定義した。

$$\alpha = \frac{a+d}{2}, \quad \beta_x = x, \quad \beta_y = y, \quad \beta_z = \frac{a-d}{2}.$$

以上から、任意の  $2 \times 2$  Hermite 行列は Pauli 行列の線形結合によって表せられることが示された。

さらに、行列  $A$  の固有値  $\lambda$  は次のような固有値方程式を解くことで得られる。

$$\begin{aligned} \det |A - \lambda I| &= (\alpha + \beta_z - \lambda)(\alpha - \beta_z - \lambda) - (\beta_x - i\beta_y)(\beta_x + i\beta_y) \\ &= (\alpha - \lambda)^2 - (\beta_x^2 + \beta_y^2 + \beta_z^2) \\ &= (\alpha + |\boldsymbol{\beta}| - \lambda)(\alpha - |\boldsymbol{\beta}| - \lambda) = 0. \end{aligned}$$

したがって、 $\lambda$  は次のように与えられる。

$$\lambda = \alpha \pm |\boldsymbol{\beta}|. \quad (\text{A.3})$$



## 付 録 B 三角形の外心

図 B.1 のように三角形 ABC の各頂点が同一円周上にあるとき, この円は三角形 ABC の外接円であり, 外接円の中心は三角形 ABC の外心 O である. 三角形 ABC の外心 O の位置ベクトル  $\vec{O}$  は次のようにして求められる. まず, 次のようなベクトル  $a, b, c$  を定義する.

$$a \equiv \overrightarrow{BC}, \quad b \equiv \overrightarrow{CA}, \quad c \equiv \overrightarrow{AB}.$$

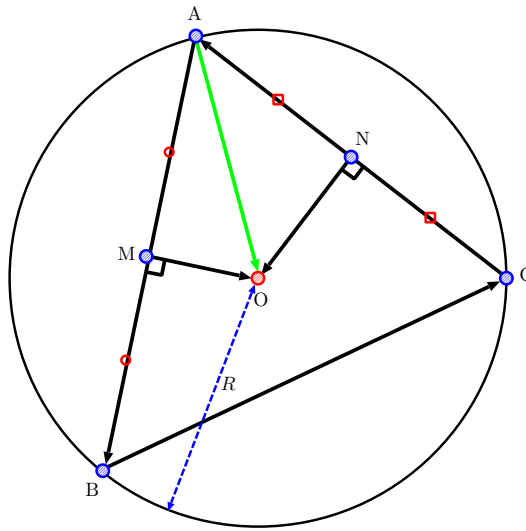


図 B.1: 三角形 ABC の外心 O

今, ベクトル  $\vec{AO}$  は次のように与えられる.

$$\begin{aligned} \vec{AO} &= s\vec{AB} + t\vec{AC} \\ &= s\vec{c} - t\vec{b}, \end{aligned} \tag{B.1}$$

ここで,  $s, t$  は実数である. また, 外心 O は三角形 ABC の各辺の垂直二等分線の交点である. 辺 AB と辺 CA の中点をそれぞれ M, N とすると,  $\vec{AB} \perp \vec{MO}$ ,  $\vec{CA} \perp \vec{NO}$  という関係が成り立つことは明らかである. まず,  $\vec{AB} \perp \vec{MO}$  という関係から, 次のような  $s, t$  に関する方程式が得られる.

$$\begin{aligned} \vec{AB} \perp \vec{MO} &= \vec{AB} \cdot (\vec{AO} - \vec{AM}) = \vec{c} \cdot \left[ (s\vec{c} - t\vec{b}) - \frac{1}{2}\vec{c} \right] \\ &= \left( s - \frac{1}{2} \right) |\vec{c}|^2 - t(\vec{b} \cdot \vec{c}) = 0. \end{aligned}$$

同様にして,  $\overrightarrow{CA} \perp \overrightarrow{NO}$  という関係から,

$$\overrightarrow{CA} \perp \overrightarrow{NO} = -\left(t - \frac{1}{2}\right) |\mathbf{b}|^2 + s (\mathbf{b} \cdot \mathbf{c}) = 0,$$

が得られる. それゆえ, 次のような  $s, t$  に関する連立方程式が得られる.

$$\begin{aligned} |\mathbf{c}|^2 s - (\mathbf{b} \cdot \mathbf{c}) t &= \frac{1}{2} |\mathbf{c}|^2, \\ -(\mathbf{b} \cdot \mathbf{c}) s + |\mathbf{b}|^2 t &= \frac{1}{2} |\mathbf{b}|^2. \end{aligned}$$

この連立方程式を解くことで,  $s, t$  は次のように与えられる.

$$s = -\frac{1}{2} |\mathbf{b}|^2 \left( \frac{\mathbf{c} \cdot \mathbf{a}}{|\mathbf{b}|^2 |\mathbf{c}|^2 - (\mathbf{b} \cdot \mathbf{c})^2} \right), \quad t = -\frac{1}{2} |\mathbf{c}|^2 \left( \frac{\mathbf{a} \cdot \mathbf{b}}{|\mathbf{b}|^2 |\mathbf{c}|^2 - (\mathbf{b} \cdot \mathbf{c})^2} \right). \quad (\text{B.2})$$

今, ベクトル  $\mathbf{b}$  とベクトル  $\mathbf{c}$  の成す角を  $\theta$  とすると, 三角形 ABC の面積  $S$  は次のように与えられる.

$$S = \frac{1}{2} |\mathbf{b}| |\mathbf{c}| \sin \theta. \quad (\text{B.3})$$

さらに, この三角形の面積  $S$  を用いた次のような関係が得られる.

$$\begin{aligned} |\mathbf{b}|^2 |\mathbf{c}|^2 - (\mathbf{b} \cdot \mathbf{c})^2 &= |\mathbf{b}|^2 |\mathbf{c}|^2 - |\mathbf{b}|^2 |\mathbf{c}|^2 \cos^2 \theta \\ &= |\mathbf{b}|^2 |\mathbf{c}|^2 (1 - \cos^2 \theta) \\ &= |\mathbf{b}|^2 |\mathbf{c}|^2 \sin^2 \theta \\ &= 4S^2. \end{aligned}$$

そして,  $s, t$  は次のように書き換えられる.

$$s = -\frac{1}{8S^2} |\mathbf{b}|^2 (\mathbf{c} \cdot \mathbf{a}), \quad t = -\frac{1}{8S^2} |\mathbf{c}|^2 (\mathbf{a} \cdot \mathbf{b}). \quad (\text{B.4})$$

したがって, ベクトル  $\overrightarrow{AO}$  は次のように与えられる.

$$\overrightarrow{AO} = -\frac{1}{8S^2} [ (|\mathbf{b}|^2 (\mathbf{c} \cdot \mathbf{a})) \mathbf{c} - (|\mathbf{c}|^2 (\mathbf{a} \cdot \mathbf{b})) \mathbf{b} ]. \quad (\text{B.5})$$

さらに, (B.5) 式から, 外心  $O$  の位置ベクトル  $\mathbf{O}$  は三角形 ABC の各頂点  $A, B, C$  の位置ベクトル  $\mathbf{A}, \mathbf{B}, \mathbf{C}$  を用いて次のように与えられる.

$$\mathbf{O} = -\frac{1}{8S^2} [ (|\mathbf{a}|^2 (\mathbf{b} \cdot \mathbf{c})) \mathbf{A} + (|\mathbf{b}|^2 (\mathbf{c} \cdot \mathbf{a})) \mathbf{B} + (|\mathbf{c}|^2 (\mathbf{a} \cdot \mathbf{b})) \mathbf{C} ]. \quad (\text{B.6})$$

また, 三角形 ABC の外接円の半径  $R$  も次のように与えられる.

$$R = \frac{|\mathbf{a}| |\mathbf{b}| |\mathbf{c}|}{4S}. \quad (\text{B.7})$$